Katharina Ziolkowski (ed.)

PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE

International Law, International Relations and Diplomacy

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

This publication may be cited as:

Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

© 2013 by NATO Cooperative Cyber Defence Centre of Excellence

ISBN 978-9949-9211-7-1 (print)

ISBN 978-9949-9211-8-8 (pdf)

ISBN 978-9949-9211-9-5 (epub)

Legal Notice:

This publication contains opinions of the respective authors only. They do not necessarily reflect the policy or the opinion of NATO CCD COE, NATO, any agency or any government. NATO CCD COE may not be held responsible for any loss or harm arising from the use of information contained in this book and is not responsible for the content of the external sources, including external websites referenced in this publication.

Copyright and Reprint Permissions:

No part of this publication may be reprinted, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the NATO Cooperative Cyber Defence Centre of Excellence (publications@ccdcoe.org).

This restriction does not apply to making digital or hard copies of this publication for internal use within NATO and for personal or educational use when for non-profit or non-commercial purposes.

Printed copies of this publication are available from:

NATO CCD COE Publications
Filtri tee 12, 10132 Tallinn, Estonia

Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org

Cover design & content layout: Marko Söönurm

Peacetime Regime for State Activities in Cyberspace

International Law, International Relations and Diplomacy

Katharina Ziolkowski (ed.)

Liina Areng
International Relations Advisor,
NATO CCD COE

Emin Çalışkan
Scientist, Research & Development Branch,
NATO CCD COE

Prof. Dr Chris C. Demchak
Cyber Conflict Studies Association (CCSA)
Co-Director, Center for Cyber Conflict Studies,
Strategic Research Department,
United States Naval War College

Prof. Dr Terry D. Gill
Professor of Military Law,
University of Amsterdam & Netherlands Defence Academy

Stefan A. Kaiser
Legal Advisor, E-3A Component,
NATO Airborne Early Warning & Control Force

Dr Jovan Kurbalija
Founding Director of DiploFoundation
Visiting Professor at the Colleague of Europe

Prof. Dr Thilo Marauhn
Professor of Public Law, International and European Law,
Justus Liebig University Giessen

Dr Martha Mejía-Kaiser
Co-Chair, Manfred Lachs Space Law Moot Court Committee,
International Institute of Space Law

Mauno Pihelgas
Scientist, Research & Development Branch,
NATO CCD COE

Dinah PoKempner
General Counsel, Human Rights Watch

Heli Tiirmaa-Klaar
Cyber Security Policy Advisor,
Conflict Prevention and Security Policy Directorate,
European External Action Service, EU

Prof. Dr Ian Walden
Professor of Information and Communications Law,
Centre for Commercial Law Studies, Queen Mary,
University of London

Oliver Aretz
Legal Assistant, E-3A Component,
NATO Airborne Early Warning & Control Force

Maj (DEU A) Dr Christian Czosseck
German Armed Forces, Bundeswehr Information Technology
Center, Head of CERT Bundeswehr Laboratory
Centre Ambassador, NATO CCD COE

Prof. Dr Robin Geiß
Chair of International Law and Security,
University of Glasgow

Prof. Dr Wolff Heintschel von Heinegg
Professor of Public International Law, European Law and
Foreign Constitutional Law, European University Viadrina
Senior Fellow, NATO CCD COE

Prof. Dr Jan Klabbers
Academy Professor (Martti Ahtisaari Chair),
University of Helsinki

Henning Lahmann
Research Assistant, University of Potsdam

Cpt (DEU AF) Markus Maybaum
Scientist, Research & Development Branch, NATO CCD COE
Researcher, Fraunhofer FKIE

Raimo Peterson
Branch Chief, Research & Development Branch,
NATO CCD COE

Dr Benedikt Pirker
Postdoctoral Researcher, European Law Institute,
University of Fribourg

Prof. Dr Michael N. Schmitt
Stockton Professor and Chairman, International Law
Department, United States Naval War College
Professor of Public International Law, University of Exeter
Senior Fellow, NATO CCD COE

Prof. Joel P. Trachtman
Professor of International Law,
The Fletcher School of Law and Diplomacy, Tufts University

Dr Katharina Ziolkowski
Senior Analyst, Law & Policy Branch,
NATO CCD COE

Table of Contents

Foreword XI
Introduction XIII
About NATO CCD COE XVI
Abbrevations XVII

PART I
INTRODUCTION TO CYBERSPACE - SOCIOLOGICAL FACETS AND TECHNICAL FEATURES

Christian Czosseck
State Actors and their Proxies in Cyberspace 1
1. Introduction 1
2. The Empowerment of Non-State Actors 3
   2.1 Hackers 4
   2.2 Organised Cyber Crime 6
   2.3 Hacktivism 7
   2.4 Industry 10
   2.5 States 12
      2.5.1 State Actor: Law Enforcement 12
      2.5.2 State Actor: Intelligence Services 14
      2.5.3 State Actor: Armed Forces 14
3. Possible Reasons for the Use of Proxies 16
   3.1 Testing New Methods while Denying Responsibility 16
   3.2 'Use' of Hacktivists and Cyber Criminals as a (Deniable) Force 17
4. A Toolbox to Build Cyber Power 18
   4.1 The 'Western Way': Capability Building and Contracting 19
   4.2 The (Better) Use of Volunteers 20
   4.3 People's War and the Inclusion of Everyone 22
   4.4 Cyber Crime as a Way to Build Cyber Power 23
5. Conclusion 24

Mauno Pihelgas
Back-Tracing and Anonymity in Cyberspace 31
1. Introduction 31
2. General Background 32
   2.1 Terminology 32
   2.2 Identification Features of Devices on the Internet 33
      2.2.1 IP Version 4 (IPv4) 33
      2.2.2 IP Version 6 (IPv6) 34
      2.2.3 Media Access Control Address 35
      2.2.4 Domain Name System 36
      2.2.5 WHOIS 37

2.3 Identification Features of Different Actors 38
2.3.1 Proficiency of the Attacker 38
2.3.2 Information from the Media and the Internet 39
2.3.3 Language and Unique Style 39
2.3.4 Unique Tools and Techniques 39
2.3.5 Action Patterns 40
3. Anonymity 40
3.1 Possible Uses for Anonymity 40
3.2 Remaining Anonymous in Online Activities 41
3.2.1 Proxy Servers 42
3.2.2 Virtual Private Network Servers 44
3.2.3 Use of Anonymity Networks (Onion Routers) 45
3.2.4 Malware Infected Zombie Computers 46
3.2.5 Concealing Personal Information 47
3.3 Challenges, Risks and Obstacles 49
4. Back-Tracing 50
4.1 Gathering Relevant Information from the Attacks 51
4.2 Tracing Attackers 51
4.2.1 The Traceroute Tool 52
4.2.2 Location of the IP Address 53
4.2.3 Determination of the Point of Contact 53
4.2.4 Enticing the Intruders into Revealing Their Identities 54
4.3 Challenges, Risks and Obstacles 55
4.3.1 Feasibility of Back-Tracing 55
4.3.2 Recovering From an Attack 56
4.3.3 Log Authenticity 56
5. Summary and Conclusions 57

Emin Çalışkan & Raimo Peterson
Technical Defence Methods, Tools, Techniques and Effects 61
1. Introduction 61
2. Information Security Objectives 61
3. ISO-OSI Model and Encapsulation 62
4. Security Applications and Devices 65
4.1 Network Devices 66
4.1.1 Switches and Routers 66
4.1.2 Firewalls 67
4.2 Detection and Prevention Systems 68
4.2.1 Intrusion Detection and Prevention Systems 68
4.2.2 Signature Based *versus* Anomaly Based Intrusion Detection Systems 69
4.2.3 Host Based *versus* Network Based Intrusion Detection Systems 69
4.2.4 Black Lists *versus* White Lists 69
4.2.5 Deep Packet Inspection 70
4.3 Honeypots 71
4.3.1 Types of Honeypots 72

4.3.2 Honeypot Solutions ... 73
4.3.3 Honeypots as a Cyber Defence Technique ... 75
5. Network Architecture and Security ... 77
5.1 Air Gapped Networks ... 77
5.2 Domain Name System Security ... 78
5.3 Cloud Computing Security ... 79
5.4 IPv6 – Solutions and Challenges ... 80
5.4.1 Background ... 80
5.4.2 Technical Insights ... 81
5.4.3 Transition to IPv6 ... 83
5.4.4 Management Issues ... 84
6. Encryption ... 85
6.1 Symmetric Encryption ... 85
6.2 Asymmetric Encryption ... 87
6.3 Limits of Encryption ... 90
6.4 Interim Conclusions ... 93
7. Organisational Aspects of Cyber Defence ... 94
7.1 Internet Organisation ... 94
7.2 Domain Name System Organisation ... 95
7.3 Information Security Management System ... 96
7.4 Secure Software Development Life Cycle ... 97
8. Summary ... 98

Markus Maybaum
Technical Methods, Techniques, Tools and Effects of Cyber Operations ... 103
1. Introduction ... 103
2. Hacking – *Mise-En-Scène* in Seven Stages ... 104
2.1 Reconnaissance – Get Information about Your Target ... 107
2.2 Weaponise – Prepare to Break the Shields ... 111
2.3 Delivery – Get the Tools to the Target ... 115
2.4 Exploitation – Hijacking the Control Flow ... 118
2.5 Installation – Reside the Payload on the Target ... 122
2.6 Command and Control – Remotely Control the Target System ... 125
2.7 Act – The System is Yours ... 126
3. Cyber Operations – A Continuous Improvement Life-Cycle ... 129

PART II
RIGHTS AND OBLIGATIONS OF STATES IN CYBERSPACE

Katharina Ziolkowski
General Principles of International Law as Applicable in Cyberspace ... 135
1. Introduction ... 135
2. Nature ... 136
2.1 Source and Content ... 137
2.2 Normativity and Categorisation ... 144
2.3 Distinctive Status within the International Law System ... 147

2.3.1 Relationship to Practice, *opinio iuris* and Consent of States ... 147
2.3.2 Higher 'Normative Value' ... 149
2.3.3 Relationship to the Concept of Fundamental Rights and Duties of States ... 152
2.4 Instrument of Progressive Law Development ... 154
3. Specific General Principles of International Law as Applicable in Cyberspace ... 155
3.1 Sovereign Equality of States and Corollary Principles ... 156
3.1.1 Self-Preservation ... 157
3.1.2 Territorial Sovereignty and Jurisdiction ... 162
3.1.3 Non-intervention in Domestic Affairs ... 164
3.1.4 Duty Not To Harm Rights of Other States (Principle of Prevention, Precaution and 'Due Diligence') ... 165
3.1.5 Principle of Good Neighbourliness and *sic utere tuo* ... 170
3.2 Maintenance of International Peace and Security ... 171
3.2.1 Refrain from Threat or Use of Force in International Relations ... 172
3.2.2 Peaceful Settlement of Disputes ... 175
3.3 Cooperation and Solidarity ... 176
4. Some Thoughts *de lege ferenda* for Cyberspace ... 178
4.1 Sustainable Development and Equitable Utilisation of Shared Resources ... 179
4.2 Common Heritage or Concern of Humankind ... 181
4.3 Protection against Globally Spreading Infections: The World Health Regime ... 183
5. Summary and Conclusions ... 184

Benedikt Pirker
Territorial Sovereignty and Integrity and the Challenges of Cyberspace ... 189
1. Introduction ... 189
2. The Notion of Territorial Sovereignty and Integrity under International Law and the Applicability of International Law to Cyberspace ... 190
2.1 Territorial Sovereignty and Integrity under International Law ... 190
2.2 The Applicable Law for Cyberspace ... 193
3. The Scope of Territorial Sovereignty in Cyberspace ... 194
3.1 The Territorial Status of Cyberspace ... 194
3.2 The Exercise of Jurisdiction and Extraterritoriality in Cyberspace ... 196
4. The Content of Territorial Sovereignty and Integrity and the Specificities of Cyberspace ... 199
4.1 Distinguishing Lower-Level Violations of Territorial Integrity from Prohibited Use of Force ... 199
4.2 Examples of Cyber Activities as Potential Violations of Territorial Sovereignty and Integrity ... 201
4.3 Territorial Sovereignty and Integrity and the Resulting Duties for States ... 203
4.3.1 Triggering the Duty of Prevention: The Role of Knowledge ... 204
4.3.2 Substantive Obligations under the Duty of Prevention: The Standard of Due Diligence ... 206
4.3.3 The Duty of Prevention and Transit States ... 209
4.3.4 Other Suggested Regulatory Approaches ... 209
5. State Reactions to Violations of Territorial Sovereignty and Integrity in Cyberspace ... 210
5.1 State Responsibility for Violations of Territorial Sovereignty and Integrity: The Problem of Attribution ... 210
5.2 Countermeasures ... 212
5.3 Necessity ... 214
6. Conclusion ... 214

Terry D. Gill
Non-Intervention in the Cyber Context ... 217
1. Introduction ... 217
2. Legal Nature and Scope of the Principle of Non-Intervention ... 219
2.1 Legal Basis of the Principle of Non-Intervention ... 219
2.2 Substantive Content and Scope of the Principle of Non-Intervention ... 221
3. Attribution of Conduct Constituting Prohibited Intervention and Possible Remedies ... 226
3.1 Attribution of Acts ... 226
3.2 Available Remedies ... 228
4. Application of the Legal Framework to Cyber Intervention ... 232
4.1 What is Cyber Intervention and Which Forms Could It Take? ... 232
4.2 Available and Possible Remedies in Response to Cyber Intervention ... 236
5. Some Concluding Remarks ... 237

Dinah PoKempner
Cyberspace and State Obligations in the Area of Human Rights ... 239
1. Cyber Communications as a Human Rights Accelerator ... 239
2. The General Application of Human Rights Law to Cyber Activities ... 243
3. Positive Obligations to Provide Access to Cyberspace ... 246
4. The Criminalisation and Punishment of Cyber Offences ... 247
5. Data Protection and Data Retention ... 250
6. Surveillance and Espionage ... 252
7. Anonymity ... 255
8. Pressuring Intermediaries: Internet Service and Content Provider Liability ... 256
9. Self-Help ... 257
10. Expanding Powers, Expanding Obligations ... 258

Ian Walden
International Telecommunications Law, the Internet and the Regulation of Cyberspace ... 261
1. Telecommunications Law ... 262
2. Cyberspace and the Regulated Sphere ... 263
3. Net Neutrality ... 265
4. International Telecommunications Law ... 266
4.1 International Telecommunication Union ... 267
4.2 World Trade Organisation ... 277
4.2.1 General Agreement on Trade in Services ... 278
4.2.2 Dispute Resolution ... 284
4.2.3 The Doha Round ... 286
5. Internet Governance ... 287
6. Concluding Remarks ... 289

Wolff Heintschel von Heinegg
Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law ... 291
1. Introduction ... 291

2. Significance and Vulnerability of Submarine Communications Cables ... 292
2.1 Significance ... 292
2.2 Threats to Submarine Cables ... 293
3. The International Legal Regime of Submarine Cables ... 296
3.1 The 1884 Convention ... 297
3.2 The 1958 Geneva Conventions ... 299
3.3 The 1982 United Nations Convention on the Law of the Sea ... 301
3.3.1 Territorial Sea and Archipelagic Waters ... 301
3.3.2 Sea Areas Not Subject to Sovereignty ... 302
3.3.3 High Seas and Obligation to Enact Domestic Legislation ... 307
3.3.4 Dispute Settlement ... 308
3.4 Preliminary Conclusions ... 309
4. Is There Insufficient Legal Protection for Submarine Cables? ... 309
4.1 (Alleged) Deficiencies of the Existing Legal Regime ... 310
4.2 Proposals for Improving the Legal Protection of Submarine Communications Cables ... 311
4.2.1 Cable Protection Zones ... 312
4.2.2 Universal (Criminal) Jurisdiction for Submarine Cable Depredations and Injuries? ... 314
4.2.3 Other Proposals ... 315
5. Clarifying the Issue of Jurisdiction ... 316
6. Concluding Remarks ... 318

Stefan A. Kaiser & Oliver Aretz
Legal Protection of Civil & Military Aviation against Cyber Interference ... 319
1. Introduction and Scope ... 319
2. Technical Background ... 319
2.1 Technical Evolution of Aviation ... 319
2.1.1 Aircraft and Automated Aircraft Systems ... 320
2.1.2 Unmanned Aerial Vehicles – Unmanned Aircraft Systems ... 320
2.1.3 Air Traffic Management ... 321
2.1.4 Communication ... 322
2.1.5 Navigation ... 322
2.1.6 Surveillance ... 323
2.2 Cyber Interference with Aviation ... 323
2.2.1 Hacking ... 323
2.2.2 Jamming and Spoofing ... 324
2.2.3 Vulnerabilities through the Supply Chain ... 325
3. Civil Aviation and Cyber Interference ... 325
3.1 Regulatory Aspects ... 325
3.1.1 Make Cyber Security Part of Airworthiness Certification ... 326
3.1.2 Adopt an Anticipating Regulatory Approach for Cyber Security ... 327
3.1.3 Avoid Commercial Off-The-Shelf Products in Safety Critical Functions ... 327
3.1.4 Limit and Secure Network Interconnection for Aircraft Systems ... 328
3.1.5 Special Solutions for Interconnection in Air Traffic Management ... 329
3.1.6 Maintain Redundancy and Diversity of Radio Navigation Systems ... 329
3.2 Criminal Law ... 330

3.2.1 The Background ... 330
3.2.2 Hague Convention ... 331
3.2.3 Montreal Convention ... 332
3.2.4 Beijing Convention and Protocol ... 333
3.2.5 National Implementation ... 334
3.2.6 Problem of Practical Application ... 335
3.3 Private Law: Liability ... 335
3.3.1 Damage Sustained On-Board ... 335
3.3.2 Third Party Damage ... 338
4. Military Aviation and Cyber Interference ... 340
4.1 The Status of Military Aircraft and National Airspace in Peacetime ... 340
4.2 Regulatory Aspects ... 341
4.2.1 Airworthiness Certification ... 341
4.2.2 Interconnection and Interoperability ... 342
4.2.3 Air Traffic Management and Military Aircraft ... 343
4.2.4 Export Control ... 343
4.3 Military Operational Law in Peacetime ... 344
4.3.1 Air Policing – Electronic Interception ... 344
4.3.2 Intelligence, Surveillance and Reconnaissance ... 346
5. Conclusions ... 348

Martha Mejía-Kaiser
Space Law and Unauthorised Cyber Activities ... 349
1. Introduction ... 349
2. Gateways for Cyber Activities ... 349
3. A Brief Look at Space Law ... 353
3.1 Regulation of Space Communications ... 354
3.2 Responsibility for Performing Space Activities ... 355
4. Liability for Damages Caused by Cyber Activities ... 356
4.1 Loss of Service and Operational Life and Destruction of Space Objects ... 356
4.1.1 Technical Background ... 357
4.1.2 Possible Scenarios ... 359
4.1.3 The Liability Convention and Loss of Service or Destruction of Space Objects ... 360
4.2 Physical Damage Caused by Space Objects in Outer Space or on Earth ... 360
4.2.1 Technical Background ... 360
4.2.2 Possible Scenarios ... 362
4.2.3 The Liability Convention and Damage in Outer Space ... 363
4.2.4 The Liability Convention and Damage on Earth ... 365
4.2.5 Recovery of Damages ... 366
5. Proposals for Legal Regulation ... 366
5.1 Prohibition of Unauthorised Cyber Activities against Space Objects ... 367
5.2 Duty to Notify the International Community of Cyber Activities against a Space Object ... 368
5.3 International Responsibility and Liability of States that Authorise Cyber Activities against Space Objects of Other States without Consent ... 369
5.4 Application of Space Debris Mitigation Measures ... 369

5.5 Adopting International Rules Banning Damaging Cyber Activities against Space Systems 370
5.6 *Res Communis* of Outer Space as a Model for Cyberspace 371
6. Conclusions 372

Joel P. Trachtman
International Economic Law in the Cyber Arena 373
1. Introduction 373
2. A Taxonomy of Cyber Operations that May Raise International Economic Law Issues 373
3. WTO Law 375
3.1 Trade in Goods 376
3.2 Trade in Services 379
3.3 Government Procurement 380
3.4 Security Exceptions 380
3.5 General Exceptions 385
4. TRIPS and Multilateral Intellectual Property Law 387
5. International Investment Law 389
6. Conclusion 392

Jovan Kurbalija
E-Diplomacy and Diplomatic Law in the Internet Era 393
1. Introduction 393
2. Impact of the Internet on Diplomacy 396
2.1 The Changing Environment for Diplomatic Activities 396
2.2 Internet Governance: A New Topic on the Diplomatic Agenda 397
2.3 New Tools for Diplomacy 398
3. Diplomatic Law 399
3.1 Status and Organisation of Diplomatic Relations 400
3.2 Core Diplomatic and Consular Functions in the Internet Era 402
3.2.1 Representation 402
3.2.2 Protection of Nationals and Consular Assistance 404
3.2.3 Negotiation 406
3.2.4 Information Gathering 408
3.2.5 Diplomatic Reporting 411
4. Immunities, Privileges and Facilities 412
4.1 State Immunity 412
4.2 Immunities of Heads of State and Government 413
4.3 Diplomatic Immunities, Privileges and Facilities 414
4.3.1 Inviolability of Hardware and Digital Assets 414
4.3.2 Freedom of Diplomatic Communication 416
4.3.3 Use of Wireless Facilities by Diplomatic Missions 418
4.3.4 Inviolability of Databases and Electronic Documents 420
4.3.5 Exemption from Custom Duties for E-Purchase 422
5. The Future of Diplomacy and Diplomatic Law in the Internet Era 422

Katharina Ziolkowski
Peacetime Cyber Espionage – New Tendencies in Public International Law 425
1. Introduction 425
2. International Law *de lege lata* 430
2.1 Illegality of Espionage 431
2.2 Legality of Espionage 437
2.3 Specific Restraints on Espionage 443
2.4 Intermediate Result: Not Forbidden or *non liquet* 445
3. New Tendencies in International Law 446
3.1 Relevance of Cyber Espionage to National Security – Reloaded 447
3.2 Emerging Interpretations of International Law 450
3.2.1 Cyber Espionage as Threat or Use of Force and as Armed Attack 451
3.2.2 Cyber Espionage as Violation of Territorial Sovereignty 457
4. International Law Policy Considerations 459
5. Conclusions 462

Thilo Marauhn
Customary Rules of International Environmental Law - Can they Provide Guidance for Developing a Peacetime Regime for Cyberspace? 465
1. An Environmental Perception of Cyberspace 465
2. Taking Stock: Sources of International Environmental Law 468
3. The Meaning of Selected Key Concepts of International Environmental Law for Cyberspace 471
3.1 The Obligation Not to Cause Significant Harm 472
3.2 The Precautionary Approach 474
3.3 Ensuring Accountability of Private Actors: The Polluter Must Pay 476
3.4 Sustainable Development 477
3.5 The Common Heritage Approach 478
4. Applying Existing Law or Making Future Law? 479
4.1 International Environmental Law as a Specialised Part of Public International Law (*lex specialis*) 480
4.2 The Transferability of Customary Rules of International Environmental Law 481
4.3 Mind the Gap! The Issue of Territoriality 483
5. Conclusions 483

Jan Klabbers
Responsibility of States and International Organisations in the Context of Cyber Activities with Special Reference to NATO 485
1. Introduction 485
2. Conceptual Issues 486
3. The 2001 Articles on State Responsibility and 2011 Articles on the Responsibility of International Organizations 490
4. Attribution and NATO 493
5. A Thought Experiment 498
6. By Way of Conclusion 504

PART III
STATE INTERACTION AND COUNTERACTION IN CYBERSPACE

Heli Tiirmaa-Klaar

Cyber Diplomacy: Agenda, Challenges and Mission 509

1. Introduction to Cyber Diplomacy – An Agenda for a Rising International Relations Sub-discipline 509
2. The Fifth Domain and Policy-Making Challenges 511
3. The Current Agenda for International Cyber Relations 517
   - 3.1 International Security and Building Trust in Cyberspace 517
   - 3.2 International Initiatives in Fighting Cyber Crime 520
   - 3.3 Capacity Building in Cyber Security and Addressing Cyber Crime 523
   - 3.4 Defending Human Rights in Cyberspace 525
   - 3.5 Controversy over Internet Governance 528
4. Mission for Cyber Diplomacy in the Future 529

Katharina Ziolkowski

Confidence Building Measures for Cyberspace 533

1. Introduction 533
2. Politico-Historic Context 534
3. Confidence Building Measures for Cyberspace 540
   - 3.1 Goals, Objectives, Tasks and the End-State Desired 541
   - 3.2 Challenges of Cyberspace 542
   - 3.3 Current Developments 545
     - 3.3.1 United Nations 546
     - 3.3.2 Organization for Security and Co-operation in Europe 548
     - 3.3.3 Bilateral Endeavours 550
     - 3.3.4 Unilateral Declarations 551
     - 3.3.5 Assessment 553
   - 3.4 Nature of the Commitments 553
     - 3.4.1 Politically Binding *versus* Legally Binding 553
     - 3.4.2 Regional *versus* Global 557
   - 3.5 Obstacles and Challenges for CBMs for Cyberspace 558
4. Significance of Political Commitments for International Law 560
5. Summary and Conclusions 562

Liina Areng

International Cyber Crisis Management and Conflict Resolution Mechanisms 565

1. Introduction 565
2. Tools and Challenges of International Cyber Crisis Management and Conflict Resolution 566
3. Global Organisations 570
   - 3.1 United Nations 570
   - 3.2 International Telecommunication Union 573
4. Regional Organisations 574
   - 4.1 North Atlantic Treaty Organization 574
   - 4.2 European Union 578
   - 4.3 Organization for Security and Co-operation in Europe 580

4.4 Collective Security Treaty Organization ... 581
4.5 Shanghai Cooperation Organisation ... 583
4.6 Organization of American States ... 583
4.7 The Association of South East Asian Nations and ASEAN Regional Forum ... 584
4.8 The African Union ... 585
5. Informal Multilateral Organisations ... 586
5.1 G8/G20 ... 586
5.2 BRICS ... 587
6. Formal Networks of CERTs ... 587
7. Conclusions ... 588

Chris C. Demchak
Economic and Political Coercion and a Rising Cyber Westphalia ... 595
1. Cybered Conflict and Systemic Offense without Military Force ... 597
1.1 Three Systemic Advantages for Cybered Offense ... 598
1.1.1 Scale in Organising ... 598
1.1.2 Proximity for Intelligence and Reach ... 599
1.1.3 Precision of Targeting, Timing, Effects and Replay ... 601
1.2 Deception and Opaqueness Key to a Cybered Campaign ... 603
2. National Power 'Cybered' in State-Level Socio-Technical-Economic System Defence ... 604
3. Cybered Coercion: 'Everyman' Shaping of Systems ... 605
3.1 Cybered Coercion: Forceless, Faceless and Fearless ... 606
3.2 Campaign Planning Questions for Coercers ... 609
4. Rise of the Cyber Westphalia ... 612

Robin Geiß & Henning Lahmann
Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention ... 621
1. Introduction ... 621
2. Cyber Security and the Military Paradigm: Self-Defence ... 621
2.1 Cyber Attacks as Armed Attacks ... 621
2.2 The Problem of Attribution ... 623
2.3 Suggestions to Alter the Legal Standards Regarding Evidence and Attribution Should Be Discarded 627
2.4 Interim Conclusion ... 628
3. Beyond the Military Paradigm: Countermeasures and Necessity ... 628
3.1 Countermeasures ... 628
3.1.1 Function and Preconditions of Countermeasures ... 628
3.1.2 Countermeasures in Response to Cyber Attacks ... 632
3.2 Necessity ... 644
4. In Search of a More Comprehensive Approach: Spelling Out States' Due Diligence Obligations in Cyberspace ... 653
5. Conclusion ... 657

Michael N. Schmitt
Cyber Activities and the Law of Countermeasures 659
1. Introduction 659
2. Countermeasures Generally 661
2.1 Countermeasures Defined 661
2.2 Countermeasures Distinguished 662
3. Conditions Precedent to Countermeasures 663
3.1 Breach of an International Obligation 664
3.2 Attribution to a State 668
4. Countermeasures Requirements and Restrictions 674
4.1 Purpose of Countermeasures 674
4.2 Situations Precluding Countermeasures 675
4.3 Restrictions on Countermeasures 678
4.4 Proportionality 682
4.5 Evidentiary Considerations 685
4.6 Originator and Target of Countermeasures 686
4.7 Location of Countermeasures 688
5. Conclusion 688

Bibliography 691
Authors´ Biographies 739

Foreword

For a considerable time now, cyberspace as a domain of military activities has been a recurring topic for diverse conferences and studies. This is also true of its sub-theme, the legal aspects of cyber warfare. Notably, in 2009, the NATO Cooperative Cyber Defence Centre of Excellence invited and hosted an independent International Group of Experts and supported their work, culminating in this year's launch of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013), a publication examining the modern cyber dimension of warfare in the traditional international law categories of ius ad bellum and ius in bello. Considering this, it now seems appropriate to make a closer examination of the more regular realm of State activities in cyberspace during peacetime.

At a time of growing global interconnectivity and increasing dependence on information and communication technology, State action without the use of cyberspace is not imaginable. State institutions themselves operate both as providers of information and services on the internet and as internet users. But even beyond these operations, States depend on available and reliable information and communication technology infrastructures: security, the functioning of vital institutions, economic and scientific progress, the organisation of social and healthcare systems, as well as the prosperity and wellbeing of the population cannot be provided without the use of cyberspace. Cyber threats that materialise in the loss of confidentiality, integrity or availability of information and communication technology can have an impact on the stability of States, in extreme cases threatening their existence. In order to minimise such risks, technical precautions certainly need to be taken; however, technical measures alone will not suffice: a solid and reliable legal framework for State activities in cyberspace is essential. The aim of this volume is to propose such a framework by identifying existing prerequisites and offering diverse interpretations, but also by pointing out unsettled issues.

One premise is certain: cyberspace cannot be deemed a legal lacuna. In this space, too, the rule of law must apply. Only then can the significance of the internet as a platform for economic and social development, but also as a contributor to understanding between States, truly unfold. However, the creation of a legal framework for cyberspace is not a task that any State could tackle alone: due to the global nature of cyberspace, an international effort is needed to find answers to questions about which rules apply to users and providers operating in cyberspace, or how access to the internet and cross-border data flow should be regulated. The international community has not yet come very far in determining a common regulatory regime for cyberspace.

The starting point for such deliberations must be norms of international law as applicable outside the digital world. Once the application of such norms in cyberspace has been clarified and the basis for an appropriate legal regime thereby established, the question of the need for new regulation will arise. Various approaches to and interpretations of international law need to be aligned in order to progressively develop a common understanding of the legal regime for cyberspace. An international scientific discourse would provide an indispensable basis for all such endeavours.

A question may be raised as to why the NATO Cooperative Cyber Defence Centre of Excellence finds it relevant to approach the topic of a peacetime regime for cyber activities and to invite internationally recognised experts to present their views and contribute to such a discourse on an international level. As proven by the range of topics addressed in this volume, even below the threshold of armed conflict, the use of cyberspace relates to significant issues in terms of military and security policy, which can be deemed of importance to the armed forces. In general terms, and apart from any particular military operations, the armed forces of modern States are affected in various ways by cyberspace: ensuring cyber security of military installations, cyber security in the field of military aviation, and the evaluation of space objects are just a few examples. In its Strategic Concept of 2010, NATO identified cyber threats as one of the emerging security challenges that the Alliance is facing. NATO's Policy on Cyber Defence of 2011 foresees cooperation with other international organisations and with partner countries for a sustainable improvement of cyber security. The legal framework governing the matters involved reaches far beyond the traditional areas of military law. Therefore, a peacetime regime for cyberspace is indisputably a matter of relevance for NATO.

From the perspective of networked thinking, a multi-disciplinary approach to the topic of a peacetime regime for State activities in cyberspace is particularly important. In general, before a certain situation can be assessed from a legal point of view, the facts of the case must be scrutinised. Therefore, before describing the rights and obligations of States in cyberspace under international law, this volume offers an overview of the technological possibilities and challenges involved. The first part of the volume explains, inter alia, the functioning of internet communications, aspects of anonymity and back-tracing of actors, as well as the methods, tools and techniques of cyber defence and cyber operations. The second and main part of the volume examines the relevance and applicability of various areas of international law to cyberspace, ranging from human rights law to consular law and from telecommunications law to environmental law. Finally, the volume provides an analysis of possibilities for reaction in response to illegal cyber activities, assessing the potential of cyber diplomacy as well as of economic, political and legal remedies as provided in the system of international relations. Thereby, the volume forms a comprehensive basis for an international discourse on a peacetime regime for State activities in cyberspace, including the respective reaction possibilities, and therefore constitutes a valuable contribution to the development of legal certainty, to inter-State confidence building and, ultimately, to the maintenance of international peace and security.

Dr Dieter Weingärtner
Director of Legal Affairs
Federal Ministry of Defence
Federal Republic of Germany

Berlin
October 2013

Introduction

Stability and security in international relations are preconditioned by predictability of State behaviour. The latter requires a common understanding within the international community with regard to the very core of applicable rules of international law, contemporary concepts of international relations and diplomatic agendas. With regard to cyberspace, the development of such a common understanding is in its early days. By offering a broad overview of the relevant topics and proposing interpretive approaches, this volume aims to bring increased clarity to this complex and important subject and to support further discussions within the international community of States.

The choice of focus on peacetime is vindicated by the fact that the vast majority of malicious cyber activities relevant to international relations occur during peacetime. Worldwide, nearly 200,000 new malware samples are identified each day;[1] governmental, commercial and private computers are being probed every minute and sometimes hacked sucessfully. Additionally, the peacetime regime for State activities is, generally speaking, not automatically suspended during times of armed conflict, but rather augmented or partly amended.[2] This applies also to governmental activities undertaken in order to 'maintain or restore international peace and security' as authorised by the United Nations Security Council under its powers pursuant to Chapter VII of the *Charter of the United Nations*.

For an interested reader who seeks to understand cyberspace and its technical components, as well as its legal, political and diplomatic implications, the present volume is the first comprehensive work providing such an insight.

To assist the reader's orientation in cyberspace, the *first part* of this volume describes, in a comprehensive but accessible way, the sociological features and technical aspects of the internet and cyberspace. It explains the activities of State actors and their proxies, technical methods for remaining anonymous online and for back-tracing hackers, common cyber defence methods, techniques and tools, and the stages of hacking computer networks. Importantly, the technical descriptions do not imply any insinuations as to the questions of legality or political acceptability of the aspects described.

The *second part* offers an interpretation of public international law with regard to rights and obligations of States in the cyber realm. The topics covered range from the notion of territorial sovereignty in cyberspace through international aviation, space and economic

---

1 cf Help Net Security, 'Nearly 200,000 new malware samples appear daily' (news, 24 June 2013) <http://www.net-security.org/malware_news.php?id=2521>.

2 Although the applicability of peacetime international law during times of armed conflict is a complex topic deserving a lengthy assessment, in general terms, it can be asserted that peacetime international law applies also during times of armed conflict, unless a particular regulation is overridden by a more specific regulation of international humanitarian law or rights and obligations of States deriving from an international treaty are suspended, be it because such a possibility is foreseen by the treaty in question (mostly requiring a formal declaration of suspension) or because the applicability of the treaty, or specific regulations contained therein, during an armed conflict is implausible. International relations concepts remain valid during armed conflict and diplomatic relations are usually not suspended.

law restrictions to matters of inter-State cyber espionage and the possible application of principles of international environmental law to cyberspace. These chapters, offering interpretations of international law as prescribing State behaviour in cyberspace, are followed by a discussion about responsibility of States and international organisations for internationally wrongful cyber activities.

The *third part* of the book elaborates on the interaction of States in cyberspace and on governments' means of counteracting malicious cyber activities. The agenda and challenges of cyber diplomacy, a due diligence standard for cyber security, the means of economic and political 'cybered' coercion, and legal remedies are presented.

The authors of the book are renowned experts selected from a wide range of backgrounds, including academia, supranational and international organisations, governmental and non-governmental entities, the civilian as well as the military sector. The diversity of disciplines as well as the international composition of the group of authors is set forth in the different citation styles used, following a selection of internationally acknowledged citation guides. Importantly, all chapters of the volume were elaborated under academic freedom.

Although summarising a volume of such dimension would be a most difficult endeavour, interestingly, three main recurring themes throughout all chapters can be identified.

First, although States are interconnected by the global internet and cyberspace, interdependent in a globalised world and unified by joint goals and obligations deriving from a myriad of international treaties and memberships in a vast number of international organisations, the world order still rests upon a structure of sovereign States and coexistence of national jurisdictions. The aspect of territoriality, specifically relevant to 'cyber infrastructure', cannot be omitted in the context of cyberspace, and a 'territorial link' of activities still shows unimpaired relevance in the realm of international law, international relations and diplomacy. In this context, the predicted rise of a 'cyber Westphalia', strengthening 'cyber boarders', relativises 'cyberlibertarian' ideals of the early days of the internet. *Second*, the anonymity of online activities and the challenges of their attribution present another common trail throughout the chapters of this volume. Anonymity may seem a curse and a blessing at the same time. It denies identification of malicious actors, thus making deterrence policies futile, the undertaking of diplomatic, political and economic reaction measures difficult, and the application of legal remedies, e.g. countermeasures, impossible. At the same time, anonymisation techniques protect businesses and their internal communications, provide the necessary opaqueness for 'cybered' coercion, allow the conduct of certain legitimate State activities, e.g. covert online observation of criminals by police forces, and enable the exercise of the human right to freedom of expression in oppressive countries. *Third*, a new general trend elaborated upon or mentioned within diverse chapters of this book is the recognition of a 'due diligence' obligation of States, either with regard to responsibility for malicious cyber activities originating from their territory, or in the broader context of a 'cyber security due diligence'.

As every large volume, this book would not have been possible to compile without the support and commitment of many others. I am indebted to the NATO CCD COE leadership and administrative staff for all of their support. I give special thanks to my colleague Kadri Kaska, an exceptionally insightful lawyer, to whom I remain most grateful for our pleasurable discussions over contents, wording and punctuation; sharing our passion for detail. Kadri's support was invaluable in the course of editing this volume and I cannot possibly praise her enough.

Last, but certainly by no means least, I would like to cordially thank all authors for their superb contributions and their pleasant cooperation. Any further appraisal is left to the reader, who can undoubtedly expect enthusing and appealing reading.

Dr Katharina Ziolkowski
(DEU-Civ)
Senior Analyst
Legal & Policy Branch
NATO CCD COE

Tallinn
November 2013

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the USA as Sponsoring Nations. The Centre is neither part of NATO's command or force structure nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member States and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-orientated interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

For information on Centres of Excellence, visit NATO's website 'Centres of Excellence' at http://www.nato.int/cps/en/natolive/topics_68372.htm.

Abbrevations

A4A ..... Airlines for America

AAC ..... Aeronautical Administrative Communications

AAIB ..... Air Accidents Investigation Branch

AAP ..... Allied Administrative Publication

ACAS ..... Aeronautical Collision Avoidance System

ACHR ..... American Convention on Human Rights

ACL ..... Access Control List

ADS-B ..... Automatic Dependent Surveillance – Broadcast

AEEC ..... Airlines Electronic Engineering Committee

AES ..... Advanced Encryption Standard

AFDX ..... Avionics Full Duplex Switched Ethernet

AfriNIC ..... African Network Information Centre

AFTN ..... Aeronautical Fixed Telecommunication Network

AIS ..... Automatic Identification Systems

AJIL ..... American Journal of International Law

AJP ..... Allied Joint Publication

Am. J. Int'l L. ..... American Journal of International Law

Am.U. Int'l L.Rev. ..... American University International Law Review

AOC ..... Aeronautical Operational Control

APC ..... Aeronautical Passenger Communication

APCN ..... Asian Pacific Cable Network

APNIC ..... Asia-Pacific Network Information Centre

app ..... approximately

APT ..... Advanced Persistent Threat

ARF ..... ASEAN Regional Forum

ARIN ..... American Registry for Internet Numbers

ARIO ..... (draft) Articles on the Responsibility of International Organizations

ARPANET ..... Advanced Research Projects Agency Network

AS ..... autonomous system

ASEAN ..... Association of Southeast Asian Nations

ASI ..... *Agenzia Spaziale Italiana* (Italian Space Agency)

ASIC ..... Application-Specific Integrated Circuit

ASLR ..... Address Space Layout Randomisation

ASR ..... Articles on State Responsibility ('Draft Articles on Responsibility of States for Internationally Wrongful Acts')

ATM ..... Air Traffic Management

ATS ..... Air Traffic Service

AU ..... African Union

BIOS ..... Basic Input Output System

BIT ..... Bilateral Investment Treaty

BNSC ..... British National Space Council

BRICS ..... Brazil, Russia, India, China, South Africa

Brook. J. Int'l L. ..... Brooklyn Journal of International Law

BSI ..... *Bundesamt für Sicherheit in der Informationstechnik* (Federal Office for Information Security, Germany)

BYIL ..... British Yearbook of International Law

C&C ..... command and control

C4ISR ..... command, control, communications, computers, intelligence, surveillance, and reconnaissance.

CA ..... Certification Authority

ca. ..... *circa*, approximately

CAPTCHA ..... Completely Automated Public Turing test to tell Computers and Humans Apart

CBMs ..... confidence building measures

CEN ..... *Comité Européen de Normalisation* (European Committee for Standardization)

CEPC ..... Civil Emergency Planning Committee

CEP RRT ..... Civil Emergency Planning Rapid Reaction Team

CERN ..... *Conseil Européen pour la Recherche Nucléaire* (European Organization for Nuclear Research)

CERT ..... Computer Emergency Response Team

CETS ..... Council of Europe Treaty Series

cf. ..... *confer*, compare

CFE Treaty ..... Treaty on Conventional Armed Forces in Europe

CIA ..... confidentiality, integrity and availability / Central Intelligence Agency

CICIR ..... China Institute of Contemporary International Relations

CKC ..... Cyber Kill Chain

CMX ..... Crisis Management Exercise

CNE ..... Computer Network Exploitation

CNES ..... *Centre National d'Etudes Spatiales* (National Space Studies Centre, France)

CNO ..... Computer Network Operation

CNS ..... communication, navigation and surveillance

CoE ..... Council of Europe

Colum. J. Transnat'l L. ..... Columbia Journal of Transnational Law

COMPASS ..... Comprehensive Approach Specialist Support

COPUOS ..... Committee on the Peaceful Uses of Outer Space

COTS ..... commercial off-the-shelf

CPNI ..... Centre for the Protection of National Infrastructure

CRSIO ..... Convention on Relations of States with International Organizations ('Vienna Convention on the Representation of States in their Relations with International Organizations of a Universal Character')

CSIRT ..... Computer Security Incident Response Team

CSIS ..... Center for Strategic and International Studies

CSM ..... Convention on Special Missions

CSNET ..... Computer Science Network

CSR ..... corporate social responsibility

CSTO ..... Collective Security Treaty Organization

CVE ..... common vulnerabilities and exposures

DARIO ..... Draft Articles on the Responsibility of International Organizations

DDoS ..... distributed denial of service (attack)

DES ..... Data Encryption Standard

DHCP ..... Dynamic Host Configuration Protocol

DISA ..... Defense Information Systems Agency

DLR ..... *Deutsches Zentrum für Luft- und Raumfahrt* (German Space Agency)

DME ..... distance measuring equipment

DMZ ..... demilitarised zone

DNS ..... Domain Name System

DNSSEC ..... Domain Name System Security Extensions

Doc. / doc. ..... document

DoD ..... Department of Defense

DPI ..... deep packet inspection

DSB ..... Dispute Settlement Body (WTO)

DSWG ..... Digital Security Working Group

EASA ..... European Aviation Safety Agency

EC ..... European Community

ECHR ..... European Court of Human Rights / European Convention on Human Rights

ed. ..... editor / edition

ed. gen. ..... editor general

EDA ..... European Defence Agency

edn. ..... edition

EEZ ..... Exclusive Economic Zone

eg / e.g. ..... *exempli gratia*, for example

EIF ..... Estonian Internet Foundation

EJIL ..... European Journal of International Law

ENISA ..... European Network and Information Security Agency

ESA ..... European Space Agency

et al. ..... *et alii*, and others / *et alia*, and other things

etc. ..... *et cetera*, and so forth / and other(s)

et seq. / et seqq. .. .. *et sequens* / *et sequentes* / *et sequentia*, and the following

ETS ..... European Treaty Series

ETSI ..... European Telecommunications Standards Institute

EU ..... European Union

Eur. J. Int'l L. ..... European Journal of International Law

EW ..... Electronic Warfare

EWCA ..... England and Wales Court of Appeal (Civil Division) Decisions

f. / ff. ..... *foliis*, and following

FAA ..... Federal Aviation Administration

FAO ..... Food and Agriculture Organization

FAZ ..... *Frankfurter Allgemeine Zeitung* (Frankfurt General Newspaper, Germany)

FBI ..... Federal Bureau of Investigation

FCC ..... Federal Communications Commission

FIRST ..... Forum of Incident Response and Security Teams

FLTSATCOM ..... Fleet Satellite Communications System

FMS ..... Flight Management System

FTP ..... File Transfer Protocol

FYROM ..... Former Yugoslav Republic of Macedonia

G8 ..... Group of Eight

G20 ..... Group of Twenty

GAC ..... Government Advisory Committee

GAO ..... Government Accountability Office

GATS ..... General Agreement on Trade in Services

GATT ..... General Agreement on Tariffs and Trade

GBP ..... Great Britain Pound

GCHQ..... Government Communications Headquarters
GDP ..... gross domestic product
GEO ..... geostationary orbit
GGE ..... Governmental Group of Experts
GPA..... Agreement on Government Procurement
GPS ..... Global Positioning System

Harv. Int'l L.J. ..... Harvard International Law Journal
HBO..... Home Box Office
HEAT..... high-explosive anti-tank (missile)
HIDS..... host-based intrusion detection systems
HTTP ..... Hypertext Transfer Protocol
HTTPS..... Hypertext Transfer Protocol Secure
HVDC..... high voltage direct current

IAA ..... International Academy of Astronautics
IADC ..... Inter-Agency Space Debris Coordination Committee
IANA ..... Internet Assigned Numbers Authority
ibid. / id. ..... ibidem, in the same place
ICANN ..... Internet Corporation for Assigned Names and Numbers
ICAO..... International Civil Aviation Organization
ICCPR..... International Covenant on Civil and Political Rights
ICJ ..... International Court of Justice
ICMP ..... Internet Control Message Protocol
ICPC ..... International Cable Protection Committee
ICLQ..... International and Comparative Law Quarterly
ICTs..... information and communication technologies
ICTY ..... International Criminal Tribunal for the former Yugoslavia
ID ..... identification / identity
IDS..... intrusion detection system
ie / i.e. ..... *id est*, that is
IEEE..... Institute of Electrical and Electronics Engineers
IETF..... Internet Engineering Task Force
IFOR ..... Implementation Force
IG ..... internet governance
IGF ..... Internet Governance Forum
IHL ..... international humanitarian law

IHLR..... international human rights law

ILC..... International Law Commission

ILM / I.L.M. ..... International Legal Materials

ILR..... International Law Review

ILS ..... Instrument Landing System

IMF ..... International Monetary Fund

IMO ..... International Maritime Organization

IMPACT ..... International Multilateral Partnership Against Cyber Threats

Int'l J. L. & Info. Tech. ..... International Journal of Law and Information Technology

Int'l L. Comm'n YB ..... Yearbook of the International Law Commission

Int'l L. Stud. ..... International Law Studies

IP..... Internet Protocol

IPS..... intrusion prevention system

IPsec ..... Internet Protocol security

IPv4..... Internet Protocol version 4

IPv6..... Internet Protocol version 6

IPX..... Internetwork Packet Exchange

ISAF..... International Security Assistance Force

ISATAP ..... Intra-Site Automatic Tunnel Addressing Protocol

ISKE ..... Intelligent Systems and Knowledge Engineering

ISMS ..... Information Security Management System

ISO/IEC ..... International Organization for Standardization/ International Electrotechnical Commission

ISP..... internet service provider

ISR ..... intelligence, surveillance and reconnaissance

Isr. L. R..... Israel Law Review

IsrSC ..... Israel Supreme Court

ISTAR..... intelligence, surveillance, target acquisition and reconnaissance

IT..... information technology

ITLOS..... International Tribunal for the Law of the Sea

ITRs..... International Telecommunication Regulations

ITU..... International Telecommunication Union

ITU-D ..... ITU Telecommunication Development Sector

ITU-R ..... ITU Radiocommunication Sector

ITU-T..... ITU Telecommunication Standardization Sector

IWG ..... informal working group

IXP..... internet exchange point

J. Air L. & Com. ..... Journal of Air Law and Commerce

J. E. Asia & Int'l L. ..... Journal of East Asia and International Law

KFOR ..... Kosovo Force

KGB ..... *Komitet Gosudarstvennoy Bezopasnosti* (Committee for State Security, former Soviet Union)

KSAT ..... Kongsberg Satellite Services

KSOR ..... *Kollektivnye Sily Operativnogo Reagirovania* (Collective Rapid Reaction Forces)

LACNIC ..... Latin American and Caribbean Internet Addresses Registry

LAN ..... Local Area Network

lit. ..... *litera*, letter

LNTS / L.N.T.S. ..... League of Nations Treaty Series

LOAC ..... law of armed conflict

LOSC ..... United Nations Convention on the Law of the Sea

M/V ..... motor vessel

MAC ..... Media Access Control (address)

MAWA ..... Military Airworthiness Authorities

MFA ..... Ministry of Foreign Affairs

MFN ..... most favoured nation

milCyberCAP ..... military cyber capabilities

MITM ..... man-in-the-middle (attack)

MIST ..... Mexico, Indonesia, South-Korea, Turkey

MIT ..... Massachusetts Institute of Technology

MN ..... marginal note

MOD ..... Ministry of Defence

MPEPIL ..... The Max Planck Encyclopedia of Public International Law

n. ..... note / footnote

N.Y. Times ..... The New York Times

NAC ..... North Atlantic Council

NASA ..... National Aeronautics and Space Administration

NAT ..... Network Address Translation

NATO CCD COE ..... NATO Cooperative Cyber Defence Centre of Excellence

NATO ..... North Atlantic Treaty Organization

NDB ..... Non-Directional Beacon

NetBIOS ..... Network Basic Input Output System

NGO..... non-governmental organisation

NIDS..... network-based intrusion detection systems

NIST ..... National Institute of Standards and Technology

nm. ..... nautical mile(s)

NNCEIP ..... Non-Nuclear Critical Energy Infrastructure Protection

no. ..... number

NPS..... nuclear power sources

NSA ..... National Security Agency

NSAU..... National Space Agency of Ukraine

NSF ..... National Science Foundation

NSFNET..... National Science Foundation Network

NSO ..... nuclear safe orbits

NSTAC ..... National Security Telecommunications Advisory Committee

NWP 1-14M..... U.S. Navy / U.S. Marine Corps / U.S. Coast Guard, *The Commander's Handbook on the Law of Naval Operations* (July 2007)

OAS ..... Organization of American States

OECD ..... Organisation for Economic Co-operation and Development

op. cit. ..... *opere citato*, in the work cited

OSCE..... Organization for Security and Co-operation in Europe

OSI..... open system interconnection

OSINT ..... open source intelligence

p. / pp. ..... page(s)

Pace Int'l L.R. ..... Pace International Law Review

para. ..... paragraph

PC ..... personal computer

PCIJ ..... Permanent Court of International Justice

PED..... passenger electronic device

Penn. St. JL & Int'l Aff. ..... Penn State Journal of Law and International Affairs

PHP..... Hypertext Preprocessor

PING..... Packet InterNet Grouper

POC ..... point of contact

PPM ..... product and production method distinction

r. / rr. . ..... rule / rules

R&D..... research and development

RAM..... Random Access Memory

RAT ..... Remote Access Tool

RBN..... Russian Business Network

RD..... Router Discovery

reg. ..... registration

Res. / RES ..... resolution(s)

rev. ..... revised

RFC..... request for comment

RFDA ..... *Revue française de droit administratif* (French Administrative Law Review)

RIAA / R.I.A.A. ..... Reports of International Arbitral Awards

RIIKS ..... *Riigi Infokommunikatsiooni Sihtasutus* (Estonian State Info-Communication Foundation)

RIPE NCC ..... The *Réseaux IP Européens* Network Coordination Centre

RIR ..... Regional Internet Registry

ROA ..... Remotely Operated Aircraft

ROP..... Return-Oriented Programming

ROV ..... Remotely Operated Vehicle

RPAS ..... Remotely Piloted Aircraft System

RPV ..... Remotely Piloted Vehicle

RRs ..... Radio Regulations

RRT ..... Rapid Reaction Team

SACEUR ..... Supreme Allied Commander Europe

San Diego Int'l L.J. ..... San Diego International Law Journal

SARPS..... Standards and Recommended Practices

SCO..... Shanghai Cooperation Organisation

S. Ct. ..... Supreme Court

SDF ..... Self-Defence Forces

SDLC ..... Software Development Life Cycle

SDR..... Special Drawing Rights

sec. ..... section

SEI ..... Software Engineering Institute

ser. ..... series

SESAR..... Single European Sky Air Traffic Management Research

SMS ..... Short Message Service

SOFA ..... Status of Forces Agreement

SQL ..... Structured Query Language

S-SDLC ..... Secure Software Development Life Cycle

SSH ..... Secure Shell

SSL ..... Secure Sockets Layer

SSR ..... Secondary Surveillance Radar

STANAG ..... Standardization Agreement

SUA Convention ..... Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

Suppl. ..... Supplement

SWIFT ..... Society for Worldwide Interbank Financial Telecommunication

Syracuse L. Rev. ..... Syracuse Law Review

Tails ..... The Amnesic Incognito Live System

TBT ..... Agreement on Technical Barriers to Trade

TCAS ..... Traffic Alert and Collision Avoidance System

TCP ..... Transmission Control Protocol

TERENA ..... Trans-European Research and Education Networking Association

TLDs ..... Top Level Domains

TLS ..... Transport Layer Security

Tor ..... The Onion Router (initially an abbreviation; term of art)

TRIPS ..... Agreement on Trade-Related Aspects of Intellectual Property Rights

TTL ..... Time To Live

Tulane Maritime L.J. ..... Tulane Maritime Law Journal

TVH ..... Thailand-Vietnam-Hong Kong

UAS ..... Unmanned Aircraft System

UAV ..... Unmanned Aerial Vehicle

UCS ..... UAV Control System

UDHR ..... Universal Declaration of Human Rights

UDP ..... User Datagram Protocol

UHF ..... ultra high frequency

UK ..... United Kingdom

UKHL ..... United Kingdom House of Lords

UN ..... United Nations

U.N.B. Law Journal ..... University of New Brunswick Law Journal

UN Charter ..... Charter of the United Nations

UN GA / UNGA ..... United Nations General Assembly

UN GGE ..... United Nations Group of Governmental Experts

UN SC / UNSC ..... United Nations Security Council

UNCLOS ..... United Nations Convention on the Law of the Sea

UNDOALOS ..... United Nations Division for Ocean Affairs and the Law of the Sea

UNEP-WCMC ..... United Nations Environment Programme – World Conservation Monitoring Centre

UNIDIR ..... United Nations Institute for Disarmament Research

UNMIK ..... United Nations Interim Administration Mission in Kosovo

UNODA ..... United Nations Office for Disarmament Affairs

UNODC ..... United Nations Office on Drugs and Crime

UNTS / U.N.T.S. ..... United Nations Treaty Series

URL ..... Uniform Resource Locator

US / U.S. ..... United States of America

USAID ..... United States Agency for International Development

USB ..... Universal Serial Bus

U.S.C. ..... United States Code

USCYBERCOM ..... United States Cyber Command

USD ..... United States Dollar

U.S. Dept. of State Bulletin ..... United States Department of State Bulletin

USS ..... United States Ship

U.S.T. ..... United States Treaties and Other International Agreements

Utah L. Rev. ..... Utah Law Review

UUVs ..... Unmanned Undersea Vehicles

v. / vs. ..... *versus*, against

Va. J. Int'l L. ..... Virginia Journal of International Law

VCCR ..... Vienna Convention on Consular Relations

VCDR ..... Vienna Convention on Diplomatic Relations

VCLT ..... Vienna Convention on the Law of Treaties

Vill. L. Rev. ..... Villanova Law Review

VMS ..... vessel monitoring system

VoIP ..... voice over Internet Protocol

vol. ..... volume

VOR ..... very high frequency omni-directional range

VPN ..... Virtual Private Network

Wall St. J. ..... The Wall Street Journal

WAN ..... Wide Area Network

Wash. Post ..... Washington Post

WCIT ..... World Conference on International Telecommunications

WHO..... World Health Organization

WiFi ..... Wireless Fidelity

WLAN ..... Wireless Local Area Network

WRC ..... World Radiocommunication Conference

WSIS..... World Summit of the Information Society

WTO ..... World Trade Organization

WWI ..... World War I

WWII..... World War II

WWW / www ..... World Wide Web

YBILC ..... Yearbook of the International Law Commission

ZLW ..... *Zeitschrift für Luft- und Weltraumrecht* (Air and Space Law Journal, Germany)

Part I

Introduction to Cyberspace - Sociological Facets and Technical Features

Christian Czosseck

State Actors and their Proxies in Cyberspace

1. Introduction

With the dawn of the Westphalian State system, States developed a perceived need to monopolise hard power, especially the use of force. While this is certainly true in the physical realm, recent times have seen States struggling as to how to secure this monopoly in cyberspace.

Power can be defined simply as 'the ability to influence others in their action' (Keller, 2012).[1] This ability also includes eluding the influence of others. States can be seen as the embodiment of this power, and their governments, of whatever kind, are the ones using this power in pursuit of national goals and ambitions. Transferring this concept to cyberspace, the term *cyber power* can be understood as the ability to act and influence through, and by means of, cyberspace.[2] Present military, economic, cultural or regulatory influence on or structures in cyberspace are at the same time the source and expression of a State's power (Keller, 2012).

In a similar way, Klimburg suggests that a State's cyber power can manifest itself along three dimensions:

1. *integrated government capabilities*, being the ability to coordinate operational and policy aspects across governmental structures,
2. *integrated system capability,* being the ability to create coherency of policy through international alliances and legal frameworks, and
3. *integrated national capability,* being the coordination of the activities of non-State actors (industry and social society) in a State and within a State's own structures (Klimburg, 2011).

Over time, States have approached these dimensions by different means and methods, and have achieved different levels of success in each of them. While States, in general, do have reasonable control over the first dimension, the second already has its limitations because of the global nature of cyberspace. Here, States are confronted with the fact that single-State approaches commonly do not achieve the necessary impact on a global scale. Global coherence is needed to solve some of the prevailing issues in cyberspace such

1 According to Keller, power can be further classified the way that *hard power* primarily resists on force and *soft power* is the use of methods like persuasion or co-option by means of diplomacy, social or economic incentives. If these two forms are combined well for a given situation, one can speak of *smart power.*

2 A more military-centric definition is provided by Kramer, Starr, & Kramer (2009), who define cyber power as 'the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power'.

as the one of (technical) attribution of (malicious) cyber activities, or the threat posed by transnational organised cyber crime, which is strongly intertwined with questions of data protection and freedom of speech. However, this coherence generally cannot be enforced by a single State on others, and common understanding as well as alliances are needed. It is especially the last dimension of 'integrated national capability' where major differences can be seen between the approaches of Western and other States. Some of these differences result from different cultures and history.

This chapter discusses ways of building State power in cyberspace, either directly, e.g., by the development of dedicated national capabilities and the use of existing elements, or indirectly by the use of proxies of different types. A proxy shall generically refer to all sorts of non-State actors, and it shall be of no significance whether a State publicly acknowledges the use of a particular proxy or not.

> [The] 'whole of nation' approach to security policy – the joint integrated application of state (whole of government) and non-state (business and civil society) efforts to attain common objectives – has only recently begun to be applied in US [United States] government circles. The West, and the United States in particular, has been relatively slow to realise the importance of integrated national capabilities in cyber power. Russia and China both have highly capable and highly visible non-state cyber capabilities that interact with their governments. (Klimburg, 2011)

Knowledge about major types of non-State actors, their capabilities and their primary motivations builds the basis for introducing the most important forms of State-use of non-State actors.

The rise of the internet to a global, seemingly borderless and, to some extent, even lawless *network of interconnected networks* gives a dramatic amplification of power to its users. As a result, some groups of non-State actors have independently acquired cyber power to an extent that they can challenge States in cyberspace. To better understand how the many groups of non-State actors emerged, it would seem helpful to point to one particular challenge in cyberspace: the difficulty in tracking a malicious activity back to its source, ultimately granting anonymity to those sources of malicious actions. This *challenge of attribution* has many reasons, the technological ones being the most pressing.

The technology and the fundamental concept of the internet as we know it today is originally based on a mid-20th century military project[3] to create a communication network highly resistant to disturbance to communication and was developed at a time when security between (and especially authentication of) communication partners was

[3] At the end of the 1970s, the *Advanced Research Projects Agency Network* (ARPANET) was one of the very first operational networks of the name giving agency, part of the US Department of Defense (Marson, 1997).

not considered necessary. With the rise of the internet, developing into a global commons enabling communication between literally everyone, cyber attacks can nowadays be launched from any place in the world.

Another reason is the easy access to anonymisation[4] and encryption technologies, as well as the rapid growth of botnets.[5] Some possibilities for back-tracing arise if the cyber attack uses means requiring a back-channel, as in cases of exfiltration of sensitive information or a command channel in case of remote control features. Also forensic analysis of seized equipment as well as reverse engineering, program style analysis or comparison of code fragments used in the malicious software (malware) can provide some indications. Still, in most cases, human mistake is the main reason for successful attribution. Another chapter in this volume is dedicated to elaborating on the technical challenges of attribution and the limitations of back-tracing.[6]

All this leads us to an unpleasant truth that a skilled and careful cyber attacker, be it an individual, a group or even a State, can conduct malicious cyber activities from anywhere, with a very small likelihood of being identified.

2. The Empowerment of Non-State Actors

Cyber actors have developed strategies or modes of operation built upon this anonymity. As a consequence, the empowerment of non-State actors has been witnessed, leveraging the global outreach and anonymity of the internet for their benefit. Hackers, (organised) cyber criminals, hacktivists[7] and, to a disputed extent, cyber terrorists, have emerged over time. To make a clear-cut distinction between them is, in many cases, futile, as globally different definitions, legal frameworks and, more often than not, political agendas lead to different assessments of the same action. In addition to this, the media shows a tendency to push their own classification of events, sometimes even against better knowledge (Farivar, 2009).

4 There are different technologies available to hide a digital identity (i.e. an IP address, a unique identifier of every ICT system connected to and enabling communication through the internet, similar to an address for postal services), by using a chain of proxies to establish a communication channel with packets riding along this chain without leaving traceable evidence. There are different ways to achieve this with the Tor software (a popular anonymisation software, which is even supported by US government in an effort to promote freedom of speech), commercial proxy providers, and the use of botnets being the most common ones.

5 A botnet, a network of robots, consists of a special malware used to infect victim systems, including the essential feature of enabling remote control over these systems via a so-called Command and Control (C&C) server maintained by the botnet's creator. If done on a larger scale (and some of them are even counting tens of millions bots), a network of hijacked systems is formed and centrally controlled by the so-called botmaster, who possesses impressive power (Czosseck, 2012).

6 See Mauno Pihelgas, 'Back-Tracing and Anonymity in Cyberspace' in this volume.

7 Hacktivism is an artificial word composed of the terms activism and hacking, and is said to be originally coined by *Omega*, a member of Cult of the Dead Cow hacker collective in 1996, describing it as 'the use of legal and/or illegal digital tools in pursuit of political ends'.

2.1 Hackers

The earlier stages of cyberspace saw the rise of so-called *hackers*; at this time, commonly younger individuals, taking an interest in *hacking*[8] into information technology (IT) services, primarily out of curiosity and the thrill of the challenge. Reputation was built by hacking into visible or noteworthy targets, commonly resulting in access to stored data on the hacked computer systems, often leaving some proof of having succeeded.

In the past, hacking was, most of the time, not a criminal act, as penal codes did not include actions describing the act or effects of hacking. Rather, if investigations took place at all, other norms, like the penalisation of copyright violation, damage to objects or sabotage, formed the basis for law suits. The wider criminalisation of these actions started around 1995, when several Western States introduced cyber crime legislation. International harmonisation efforts are few in number, the *Convention on Cybercrime* (Council of Europe, 2001) being one of the most significant.[9]

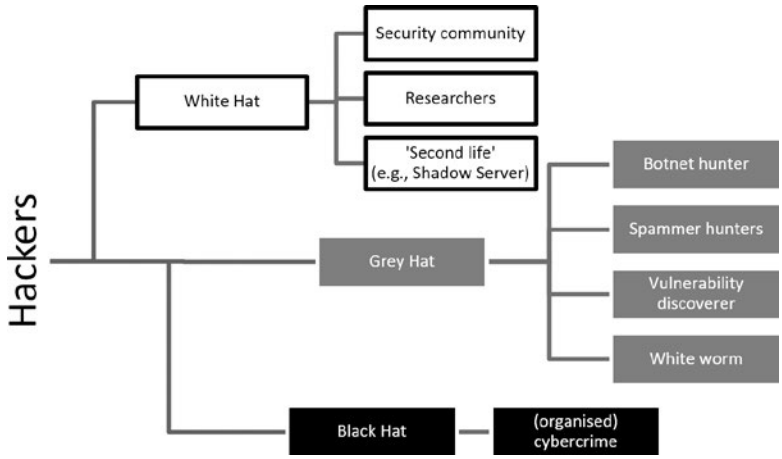

Figure 1. The evolution of the hacker community.

Over time, the hacker community evolved into three major directions, as illustrated in Figure 1. The community still exists, but the ideals and driving factors might have changed and it is now difficult to make a clear-cut distinction between the different groups.

8 Breaking into computer systems by circumventing security mechanisms (if actually in place) or the use of vulnerabilities in the architecture or in products used in forming this computer system. Depending on the ICT system at hand, the necessary skills for a successful hack can vary over the full spectrum from simple to highly sophisticated.

9 As of June 2013, all but two members of the Council of Europe have signed the conventions, with 11 not having ratified it yet. A few other States, most noteworthy Australia, Japan and the US, have also ratified it (Council of Europe, 2013).

Often, hackers without a malicious intent are referred to as *white hats* or *ethical hackers*.[10] With information and communication technology (ICT) and services becoming a global market, securing those systems and services from all sorts of malicious activities also became a lucrative profession, encouraging many to specialise in this area. Hacking nowadays also refers to a particular skillset, which many in the computer security business acquire to help protect customers from malicious actors. So called penetration-testers (commonly shortened to 'pen-tester') test and challenge ICT security mechanisms for their clients, with the ultimate goal of assessing and helping to improve the level of security and resilience. Other technical security experts are commonly required to have at least a basic understanding of hacking techniques in order to have a solid grounding in the threats they are expected to deter. Many universities already include some levels of hacking education into their curricula of IT-related studies, and researchers study these methods from a scientific point of view.

The second group which emerged is called *grey hat*s. These hackers often want to support the wider community, making cyberspace more secure by using their skills against wrong-doers. As they are doing it without proper authorisation and generally without the consent of the targets of their actions, their behaviour can sometimes be regarded as criminal; however, the grey hats justify their activities with the higher good they want to achieve. An example is grey hats taking actions against botnets by trying to infiltrate them and ultimately taking them down. Botnets are commonly regarded as one of the major global threats and central instruments for most of the malicious activities from which internet-connected parties are suffering (Plohmann, Gerhards-Padilla & Leder, 2011). If the infiltration of the botnet command and control infrastructure is successful, one can take over a botnet and try to identify all the infected victims of the botnet, with the aim of later informing them of the fact that their computers were infected (Leder, Werner & Martini, 2009). Alternatively, an uninstallation of the malware from the infected computers could be initiated and a patch distributed so that a later re-infection might be prevented. As all these actions would require access and manipulation of another's computer systems (without their consent), it is in most cases regarded as a criminal act, and leads to further liability questions in case the disinfection process shows side effects. Another example of grey hat activities is to challenge the security of (random) companies by hacking into their computer systems and often also declaring their success publicly. But, in contrast to hackers with malicious intent, grey hats contact their victims, informing them that they had a vulnerability in their IT defence. The grey hats might even share the necessary information as to how to eliminate these vulnerabilities for good.

10 The International Council of Electronic Commerce Consultants is the self-described world leader in IT security courses, which established and successfully markets the Certified Ethical Hacker programme to train security experts in the arts of hacking for public good (EC-Council, 2013).

Others use such knowledge to blackmail their victims, which leads into the last subculture of hackers introduced here, often referred to as *black hat*s.[11] Members of this community use their skills and knowledge primarily for personal gain, from earning a reputation for having done something of (malicious) significance, to illicitly earning money by stealing information of importance or blackmailing others by denying services important to them.

2.2 Organised Cyber Crime

Around the end of the 20th century, because of major investments and successful improvements in IT security, the level of skill required to successfully penetrate the security of protected ICT systems increased dramatically. Furthermore, because of an increasing number of people connected to the internet, many of them with a relatively low level of ICT security awareness and often without appropriate protection, organised cyber crime emerged, taking advantage of especially the latter group, and this changed the game dramatically.

The lack of attribution and the transnational nature of cyber crime, in contrast to the limited introduction of cyber crime legislation worldwide and (consequently) the limited international cooperation in cyber law enforcement, encouraged the formation of globally operating, organised cyber crime, which generates revenue of tremendous magnitude. For example, the United Kingdom (UK) economy alone is said to suffer from 27 billion GBP in damages and losses per year from cyber crime (UK Cabinet Office & Detica Ltd, 2011). Others estimate the damage done to individuals globally to be 388 billion USD annually (Symantec, 2011).[12]

One of the most famous global cyber crime organisations used to be the Russian Business Network (RBN), which was considered 'the baddest of the bad' by the journal *The Economist* (2007), and has been the only cyber crime organisation so far to be recognised as a major threat by the North Atlantic Treaty Organization (NATO) (*The Daily Beast*, 2009). Back in 2007, RBN accounted for approximately 40% of the global cyber crime turnover, considered to be more than 100 billion USD (Klimburg, 2011).

What makes organised cyber crime important, and this is shown with the example of RBN, is that for quite some time they had been the *de facto* provider of all sorts of

11 Despite the similarity in names, the well-known 'black hat' conference is a legitimate event, which 'bring[s] together thought leaders from all facets of the infosec world – from the corporate and government sectors to academic and even underground researchers' (black hat, 2013). Most of them would not be classified as black hats in the sense presented here.

12 Measuring the cost of cyber crime highly depends on which costs – criminal revenues, direct or indirect losses and defence costs – are taken into consideration and, as such, the sum can vary significantly depending on the concrete choice made. Levi (2012) provides a very detailed breakdown of these costs by type.

tools, technologies and intelligence[13] necessary for malicious cyber activities, such as malware,[14] exploitation packs,[15] rootkits[16] or botnets to name a few. Over the last two decades, an underground economy evolved where anyone interested was able to acquire the latest malware technology, or even services, from cyber criminals for a relatively low fee. Many of these products come with licence schemes, infection guarantees, update services and 24/7 support lines, bringing the barrier to enter the realm of cyber crime down to a level where even individuals with limited knowledge about computer science or hacking can join in (see, e.g., the example of the Russian underground market in Goncharov, 2012).

2.3 Hacktivism

The availability of this malicious technology is an enabler for another group of actors: *hacktivists*. In contrast to cyber criminals, hacktivists, who are commonly individuals or groups of individuals, conduct cyber attacks primarily for political reasons rather than monetary ones (Denning, 2001; Ottis, 2010). Hacktivists tend to select targets with high visibility which they see as appropriate to deliver the intended political message. As for the commonly missing monetary incentive in target selection, organisations from the public or private sector alike are likely to become victim to hacktivist attack campaigns, often being hit unprepared (Czosseck, Ottis & Talihärm, 2011). As a preferred method of choice, launching Distributed Denial of Service (DDoS)[17] attacks to deny internet-connected services or defacing[18] websites are the two most commonly seen techniques.

Looking at the skills present with individual hacktivists, it is difficult to make a general assessment. The level of skill and internal organisation (including command and control) varies greatly between the various groups of hacktivists seen so far.

Offering a more generic approach, any hacktivist group might display the following characteristics. In most cases, some form of a core unit is present, giving the whole group its mission, setting the aims, and often executing a certain degree of control over

13 This is true in particular for the discovery of vulnerability in software products necessary for the development of exploits to circumvent security mechanisms.

14 Malware, an artificial word for malicious software, commonly refers to software developed and deployed to conduct malicious actions, such as stealing sensitive information or abusing infected computers by making them part of a botnet.

15 An exploit is the part of malware developed to penetrate a victim's computer security by abusing a known vulnerability. The cyber crime underground market offers stand-alone software bundles to automate the act of exploitation and sells it in form of so-called exploit kits, often with update services and support channels.

16 Rootkits are a special type of malware to establish a persistent and undetectable foothold in an infected computer system.

17 Distributed Denial of Service (DDoS) attack is a method commonly applied by the use of botnets to create vast amount of traffic and direct it to a victim ICT system to the end that this system is overwhelmed and does not operate properly, effectively denying access to the service provided by the attacked system.

18 Web defacement is an act of hacking: a website is accessed and parts of it changed to the extent that, e.g., pictures or messages of offensive or political nature are shown without the consent of the website's owner.

the rest of the hacktivist group. At least some members of this core group show decent technical skill to the extent that they can (from a technical viewpoint) select meaningful digital targets, identify vulnerabilities for exploitation within them, and prepare sets of tools for the whole group to conduct cyber attacks. Sometimes they even prepare automated attacks to the extent that they are easy to use by everyone, e.g., by merely clicking on a link or on a button provided on a website (*clicktivism*).

Around these central groups and their ideas or campaigns, supportive minds would join in the activities. Here the spectrum can start with technically unskilled 'followers', who basically use the prepared and distributed tools[19] against the targets which have been pre-selected.[20] At the other end of the spectrum, highly skilled people join, using their skills to conduct their own exploitation and even extend the initially prepared set of tools and attack vectors, opening up new options to the whole group. Sometime even subgroups form, starting related but independent actions on their own. Here, the circle may start again.

Despite the fact that cases of hacktivism had already been seen,[21] the following developments can be named as fuelling the massive raise in hacktivist activities witnessed over the last few years.

- The cyber attacks against Estonia in 2007 (see, e.g., Nazario, 2009) followed by intense media attention around this particular incident, classifying it as the first 'cyber war' in human history (Landler & Markoff, 2007), created a cyber war hype (Farivar, 2009). While the facts about this incident were not always correctly reported,[22] this event made the point that a massive uprising of mere citizens can indeed have an impact that a State might recognise as a national security incident.
- The rise of Anonymous (McLaughlin, 2012; Pras, Sperotto, Moura & Drago, 2010), including its offspring LulzSec, needs to be mentioned: united in the goal of protecting the freedom of access to information and fighting all those who are seen as challenging this right, they created a global community for those

19 Anonymous is frequently distributing and using a tool called *Low Orbit Ion Cannon* for conducting service-denying cyber attacks; it is a simple tool (its name is referring to a certain weapon in the computer game *Command & Conquer*) where, after entering a target's IP address, all that is needed to execute the attack is to hit the 'IMMA CHARGIN MAH LAZER' button.

20 Anonymous, for example, is communicating its attack campaigns with pictures showing the IP addresses of the pre-selected targets.

21 Early incidents include, e.g., the WANK computer worm used against NASA in 1989 (in protest of the Galileo space probe, which was fuelled with radioactive plutonium), the Portuguese hacking group UrBaN Ka0s hacking official websites of the Republic of Indonesia in 1997 (taking a stand for East Timor's freedom) or the 'cyber war' between US and Chinese hacking communities in 2001 (following a Chinese-American plane collision).

22 It is often claimed that, under the pressure of cyber attacks, namely DDoS attacks, the State of Estonia was disconnected from the internet. In fact, Estonia, because of the fact that most of the relevant national services were provided in the country itself, decided to disconnect from the internet by denying all incoming traffic and successively re-established connection allowing only known good traffic to enter the country. Observed from outside Estonia, this gave the impression of Estonia being disconnected (Tikk et al., 2010).

supporting that idea. Besides a hard core of supporters who share the general vision of Anonymous, many more are joining individual campaigns, depending on whether they share the reasons behind the current campaign or not. Others are just joining, based on available time or to be part of something greater.

- Another influential development can be seen in the introduction and rapid grow of social networks like Twitter and Facebook, allowing an effortless global outreach for everyone able to open a social network account and having enough followers. Never has it been this easy to reach out to millions of people to make a statement. It should be noted that it is difficult to draw the line between hacktivism as a form of civil expression of political option (similar to a sit-in in the real world) and the thrill of being part of a criminal action without the risk of being identified. Sometimes it is, in the end, a political call, allowing a State to respond to such an incident appropriately from no action all the way up to the most severe consequences for the involved individuals.
- Another group worth being briefly introduced in this context is WikiLeaks. While their methods are clearly different from those used by Anonymous, as they do not deny access to internet services or deface websites to express a political opinion, they share the core idea that the public should have the right to access (sensitive) information. As such, making stolen documents available to a wider public, as seen in the disclosing of 250,000 US embassy cables in 2010 (Leigh, 2010), can be regarded as a form of making a political statement.

The real level of impact these actors have on States is debatable. Opinions range from being primarily annoying without any substantial impact besides media attention, to hacktivism manifesting as a new actor outside of direct State control, representing a decent amount of soft power, enough to even influence States.

With regard to the economic impact, the so-called Operation Payback, against VISA et al., gives an idea as to how serious the impact can be. In response to WikiLeaks publishing 250,000 classified United States (US) documents, different banks cancelled their service contracts with WikiLeaks with questionable supporting arguments, as the US was applying pressure to not support WikiLeaks, which was financed by donations. Anonymous stood up to this, launching Operation Payback against, among others, VISA, PayPal and Post Finance (Correll, 2010a). In the end, the targeted companies suffered from more than 37 days of downtime of their internet-connected services in total (Correll, 2010b).

Going even further, the leak of classified documents is said to have been a crucial trigger for the events in Tunisia in 2011. For some time, Tunisian citizens had been dissatisfied with their government. The negative comments of US diplomats regarding Tunisian officials, which were revealed by this process, put oil on the fire of these critical voices. The State responded to this by means of censorship, which then brought Anonymous to the stage, launching a DDoS and defacement campaign against the government and

some private companies, in support of these critical voices (Ryan, 2011a). Some argue (and Anonymous claims) that this chain of events and the involvement of hacktivists (primarily Anonymous) might have played a central role in the events to follow, ultimately ending in the Arab Spring movement with all effects yet to be seen (Ryan, 2011b). However, the majority opinion seems to be that the root cause for the events in Africa lies in the societal and governmental issues, such as unemployment, corruption, aging dictatorships or the contagion effect (Manfreda, 2011).

2.4 Industry

The development of the internet was a key driver for the globalisation of economies. At the same time, the increasing demand for, and access to, internet-based services was a driver for industry to invest into the global ICT infrastructure, and to build many more local networks, resulting in a cycle of demand and growth.

With regard to this process, one should acknowledge that it is the private sector which owns most of the global communications infrastructure, with the exception of countries where the national internet service providers are State-owned or at least State-controlled. In addition to this, an overwhelming majority of all products and services related to this infrastructure are developed, produced and provided by the industry.

States do have a reasonable influence over ICT companies, which is twofold. On the one hand, States have regulatory power, and can enforce compliance with rules and laws they pass. On the other hand, they have a reasonably large influence on industry because of their own purchasing power. This is amplified if groups of States, such as member States of NATO, are looking to harmonise their (military) ICT systems and, with this, set standards for other States in the group to follow.

While self-developed software was more widespread in the second half of the last century, budget constraints and the need for interoperability and standardisation encouraged many States to turn to industry for *commercial off-the-shelf* (COTS) products with little to no customisation. For example, for weapon technology, nowadays it is not the State but the specialist industry which is at the cutting edge of science and development, and States are becoming their (privileged) customers.

As a consequence of this development, it is again the industry which has a *de facto* monopoly on the ICT defence technology used to protect cyber assets from cyber attacks all over the world.[23] It is also the industry which, in this process, gained access and accumulated a tremendous amount of intelligence data, and derived from it knowledge

[23] To illustrate this with one example: the global market for malware protection software is divided among 30 to 40 companies (ShadowServer, 2013), of which seven companies hold nearly 80% of the market share (OPSWAT, 2012). The fact that currently nearly 200,000 new malware samples are discovered each day (Help Net Security, 2013) gives the impression of the very high barrier to overcome for anyone interested in establishing similar capabilities.

about all sorts of cyber activities, primarily with a focus on malicious actions. All key players in the IT (security) industry, such as Microsoft (as the world dominant operating system provider for end-user computers), Cisco (as the most important supplier of network devices), all major providers of malware protection products[24] and volunteer organisations like Shadow Server,[25] have built up their own global sensor networks to detect, collect and analyse malware, and to identify sources of malicious actions. Cisco claims to be able to see and analyse about 70%[26] of all global internet traffic, thus disposing of an extraordinary basis for gathering intelligence on all sorts of activities on the internet. By this, such industry actors became an important source of information, and States might be assumed to take advantage of this.

Turning attention to the means and actions more relevant to offensive cyber activities, industry has a long history of corporate espionage. While it would go too far to say that it is common practice, it is still safe to assume that there has always been a decent number of industry actors who leveraged different methods and levels of intelligence work in an effort to acquire information about, e.g., intellectual property, business strategies and price offers in bidding situations, ultimately to acquire a competitive advantage. As with State espionage, the increasing penetration of ICT into every aspect of modern society has enabled new ways of conducting espionage, maybe even with less risk, considering the problem of attribution elaborated above.

With the growing understanding within the public with regard to the importance of ICT security, the increasing need to defend against the growing stream of cyber attacks, and the start of the global cyber war hype accelerating this process even more, industry increasingly started to deliver 'special services' which, in their very technical nature, are quite similar to that which the cyber crime underground market is providing.

The recent increase in companies offering pen-testing services might serve as an example of this. Another might be the deployment of custom malware for, e.g., law enforcement purposes. An industry[27] has formed to which States can turn and request the development of special software intended for lawful interception of communication

24 Commonly referred to as anti-virus software, these products nowadays come as a suite of different technologies bundling together malware detection, intrusion detection and prevention, firewall functionality and reputation systems.

25 'Established in 2004, The ShadowServer Foundation gathers intelligence on the darker side of the internet. We are comprised of volunteer security professionals from around the world. Our mission is to understand and help put a stop to high stakes cybercrime in the information age.' (see https://www.shadowserver.org/wiki/).

26 Stated by Mr John Stewart, Senior Vice President and Chief Security Officer at Cisco Systems in his key address on the occasion of the NATO Information Assurance and Cyber Defence Symposium 2013 in Mons 17-19 September 2013.

27 Gamma International is one of the well-established companies in this field. Its Chief Information Officer (CIO) at the 4th International Conference on Cyber Conflict, in Estonia 5-8 June 2012, explained that the company maintains a decent catalogue of vulnerabilities and suitable exploits so that it is able to bug literally every device commonly available. He further explained that his engineers spend roughly 20% of their time fabricating the desired custom malware, but have to spend the remaining 80% of their time ensuring compliance with the relevant legal regime and, if applicable, the relevant court order to ensure the lawfulness of use.

conducted over the internet.[28] Other States might also leverage such services in the context of State espionage. From a technical standpoint, this software is *de facto* malware, using the very same technique to infect, hide and operate as the one produced by organised cyber crime for their purposes.

A last domain where industry has developed a lucrative legal market, and where cyber crime had already established an illegal one, is the discovery of vulnerabilities and suitable exploitation. Many of the more sophisticated cyber attack methods require knowledge about vulnerabilities in a product used in the victim's ICT environment, combined with the capability to 'weaponise' this vulnerability by the development of a so-called *exploit*. The more widespread and the more securely written a product is, the more valuable the discovery of a yet unknown vulnerability in these products becomes. For these so called zero-day exploits prices are said to be between 30,000 USD and 250,000 USD to anyone willing to exclusively sell their knowledge; sometimes even higher prices are being reported. In this industry different business models emerged like the one of a broker acting as a platform or reseller. Others are specialized companies establishing a business by developing their very own zero-day exploits and selling them to their customers. Many companies and governmental services are said to hold subscriptions to such companies just for the right to look into their catalogue and buying from it (Greenberg, 2012).

2.5 States

Looking at States as actors in cyberspace, there are three major fields of activity commonly seen among all States.

2.5.1 State Actor: Law Enforcement

To ensure internal security is one of the fundamental goals of most States, which commonly includes enforcing the rule of law or protecting citizens from crime. For most internet-enabled countries, this naturally includes the enforcement of law also in cyberspace. As technology evolves and enables new possibilities, the same is true for crime and its adaptation to this development as already elaborated.

While up to the end of the 1990s, cyber crime had not received much attention compared to other forms of crime, times have changed to the extent that, e.g., the US Federal Bureau of Investigation (FBI) ranks the objective to '[p]rotect the United States against cyber-based attacks and high-technology crimes' third in their 2013 priority list, immediately after the protection from terrorism and foreign intelligence efforts (FBI,

[28] It needs to be noted that most classical land line communication nowadays is in fact digital, routed over the very same infrastructure as other internet communication.

2013). It is safe to assume that most States with decent ICT penetration have, by now, set up dedicated structures to investigate cases of cyber crime.

For most of these law enforcement structures, *computer forensics* and *open source intelligence* capabilities are likely to be taken for granted. The need to intercept (also encrypted) communication required many States to find technical and legal solutions beyond simple wiretapping.[29] One way is to use the regulatory power States possess over industry operating in their national markets, and legally require unencrypted access to encrypted data.[30] Another might be the use of special software to intercept the communications already on the devices used by the culprits. This often requires the development of software with the same attributes as malware and, as such, knowledge and skills commonly not present in law enforcement agencies. As a consequence, these agencies sometimes turn to specialised companies[31] on the market to write such software. Other States are known to have built up their own capabilities to develop such software.[32]

In its fight against the challenges posed by anonymisation technology such as Tor[33] when used by serious criminal elements (e.g. child pornography traders), the FBI recently took over a hosting service provider which was under suspicion of supporting this type of crime. The website service was manipulated in such a way that the computers of individuals browsing to this site using anonymisation technology became infected by a small piece of well-crafted malware, a *modus operandi* commonly used by cyber crime actors. This malware then sent information back to the FBI, enabling later identification of these persons. This underlines that, in the fight against crime conducted by and with cyber means, law enforcement agencies might use the very same technologies and methods as cyber criminals but, of course, with proper legitimacy, aiming for different purposes. The same notion of dual use becomes evident when turning to State-level espionage.

---

29 Since the days of analogue communication, this is a standard routine for law enforcement agencies and most States have established a legal basis to request support by telecommunication service providers if certain legal requirements are met. Nowadays, the same is possible and required from telecommunication and internet service providers, but the widespread use of encryption technology or distributed ways of communication like Skype requires different approaches than just copying traffic.

30 See the example of Saudi Arabia and India vs. Blackberry, a company which entered the market with a promise to its customers that all communication and messaging would be protected from eavesdropping by everyone, including States. These States denied Blackberry's new service access to their national markets (Emigh, 2010).

31 Besides the given example of Gamma International as a company dedicated to providing law enforcement agencies with solutions to aid their investigations, there are many other companies doing the same, such as the German Digi Task GmbH, which developed for the Bavarian State Police a program capable of intercepting voice over IP and Skype communications as well capturing keystrokes and screen shots (Voß, 2011).

32 The FBI has a longer track record of the development of tools and systems to lawfully intercept communication, among them Carnivore, deployed around 2000 and replaced since (McCullagh, 2007).

33 Tor is a free software intended to enable online anonymity by directing internet traffic through a voluntarily built, free global network to conceal a user's location or access to internet services from anyone conducting network surveillance. In its initial stages, it was sponsored by the US Naval Research Laboratory.

2.5.2 State Actor: Intelligence Services

Espionage between States is a common and rather traditional activity which is an internationally accepted State practice, even if the act as such is generally criminalised in national legal systems. Intelligence agencies commonly leverage all means and methods to acquire the desired information (Lewis, 2010; Pelican, 2012; Reuters, 2012).

With the global development of society towards the inclusion of ICT, intelligence services were provided with a new set of possibilities to reach their aims. As for the relatively safe and global outreach of espionage actions via the internet, many States rapidly developed capabilities to operate in and via cyberspace, as well as to intercept data sent over the internet, or broadly to spy on the internet looking for activities of interest.

While public information about concrete capabilities of intelligence agencies is very limited, the recent scandal initiated by Edward Snowden concerning the alleged actions taken by the National Security Agency (NSA), enabling them to get access to all sort of data stored in, or passing by, US territory and to decrypt most of this data if necessary[34], serves as a good illustration of what States with a decent budget and enough soft power can achieve in this domain. Another example of the use of recognised ICT experts is illustrated by the five year contract between the NSA and a world famous hacker and security expert, Charlie Miller.[35]

2.5.3 State Actor: Armed Forces

Speaking about cyberspace as a battlefield and the development of military capability requires a comment about the current cyber war rhetoric commonly used by the media since the Estonia incident in 2007. In an indiscriminate manner, the term 'cyber war' refers to all sorts of malicious activities in cyberspace, giving little attention to the established meaning of the term *war*, but rather increasing attention to the news to be told by the press (Farivar, 2009).

In all cases seen so far, a 'cyber war' (relying solely on means effective in cyberspace), in the meaning of an 'armed conflict', has not taken place (Lewis, 2010). From a legal point of view, the actions taken by individuals or groups of individuals have to be classified as

34 According to the documents and information leaked by Snowden, the NSA '[…] have focused on compromising encryption found in Secure Sockets Layer (SSL), virtual private networks (VPNs) and 4G smartphones and tablets. The NSA spent $255 million this year on the decryption program […] which aims to "covertly influence" software designs and "insert vulnerabilities into commercial encryption systems"' (Winter, 2013). In the course of developing the global surveillance system *Prism*, major US companies, and some of the most important global companies to provide widely used services and products, such as Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube and Apple, have been forced to allow NSA direct access to their data (Poitras & Gellman, 2013).

35 Charlie Miller is considered one of the world's best hackers and earned considerable recognition for these skills in repeatedly breaking into Apple products in public competitions.

acts of cyber crime, which mostly also includes cases of hacktivism. Even in the often referred to case of the cyber attacks against Estonia in 2007, Estonia's official view of these events has been that this was an act of crime rather than war (Tikk, 2009).

The earliest case of State use of cyber means against another State reportedly took place in 1982, when a logic bomb was supposedly placed in a gas drilling equipment at a time when the US assumed the KGB[36] was stealing US drilling technology and equipment for the sake of their own gas production. This ultimately led to the largest non-nuclear explosion ever seen so far in Siberia (Russell, 2004; Safire, 2004). Furthermore, during the first Iraq war, the US supposedly made preparations for cyber attacks along with conventional operations, but never executed them because of the fear of unpredictable side effects (Markoff & Shanker, 2009).

The probable first known case of an international conflict of a kinetic nature combined with methods of warfare in cyberspace was the international conflict between Georgia and Russia in 2008. The conventional operations seemed to be coordinated with actions in cyberspace, even though they were conducted by cyber criminals and hacktivists (Tikk, Kaska & Vihul, 2010).

The events in Estonia and Georgia were a major stimulus to the discussion as to how to use cyberspace as a domain to engage with, and defend against, an adversary. But not all States recognise cyberspace as an independent warfare domain, arguing, for example, that, while ICT is an essential part of most modern (weapon) systems and, as such, shows a high level of interconnection to all other warfare domains, it does not have the independent nature to stand on its own (Keller, 2012). One might disagree with this viewpoint that there are possible ways to project power upon someone else only via cyber means. In the end, it is up to the States to establish their position and act appropriately, as done, for example, by the US and Canada, which officially declared cyberspace the fifth warfare domain (Starr, Kuehl & Pudas, 2010).

Even without the need to officially recognise cyberspace as a warfare domain, it is beyond doubt that States are under pressure to develop military capabilities to operate in cyberspace, to the extent that scholars have compared current State behaviour in and about cyberspace with past cases of arms races, seeing strong signs of a new race starting (Jellenc, 2012).

While at the beginning of the 21th century, only a few States[37] were publicly known to have started to develop military cyber capabilities, in 2011, as the research by the United Nations Institute for Disarmament Research shows, about 32 States have included cyber warfare in their military planning and organisations (UNIDIR, 2013). The US, China

36 The KGB, usually translated as Committee for State Security, used to be the main security agency for the Soviet Union until the country's collapse in 1991.

37 Billo and Chang (2004) offer a comparison of the cyber doctrines or equivalent documents for China, India, Iran, North Korea, Pakistan and the Russian Federation as far as back as 2004.

(Fritz, 2008; Kanwal, 2009; Krekel, Bakos & Barnett, 2009; Perry, 2007) and Russia (Giles, 2011, 2012) are well known and commonly recognised for having developed cyber warfare capabilities.

3. Possible Reasons for the Use of Proxies

One of the reasons for States' use of proxies can be motivated by the lack of, or limited access to, the technology and skilled individuals needed for States to build decent cyber capabilities. Considering the current market situation where those with decent skills and knowledge necessary to defend against sophisticated attacks or to conduct operations in cyberspace are limited in number, States find themselves in direct competition with industry for attracting such personnel, with the latter commonly offering salaries States find hard to match. Additionally, the hunt for exploitable vulnerabilities necessary for conducting intrusive cyber operations is an expensive road to go down. At the same time, discovering these vulnerabilities and fixing them before they are 'weaponised' by others is an important activity for defenders of high security environments. Ways of building a State's cyber power as a combination of a State's own capabilities and those of non-State actors will be elaborated upon later in this chapter.

One could think of further motivations for States to consider turning to proxies. This might be the case if, e.g., a State does not have any relevant cyber capabilities to achieve the desired effects in cyberspace. Also, States might hope for proxies to conduct operations in cyberspace independently from State's own elements. The following will introduce some theoretical reasons for States considering this option without pointing to any particular one.

3.1 Testing New Methods while Denying Responsibility

A solution to the current challenge of technical attribution of malicious cyber activities might need a global effort which seems unlikely to happen any time soon. Some even argue that improved regulation of cyberspace might not be favoured by States today, as a more or less unregulated cyberspace gives them more room to explore new ways of projecting power, ultimately supporting their goals (Fritz, 2008). The lack of worldwide implementation of cyber crime legislation and the deficiencies of international cooperation in cyber law enforcement actions are some of the crucial issues facilitating the prevailing threat by organised cyber crime and the threat of hacktivism.

Under these circumstances it is theoretically possible to think of a State, or a sufficiently influential non-State actor, to choose a proxy to execute a cyber operation in its place, with the strategic goal of testing the level of quickness, efficiency and coordination of the defensive actions taken by the victim and the international community in general.

The Conficker botnet could serve as an example for this approach. In November 2008, a sophisticated malware which combined many of the most advanced malware and botnet

technologies present at that time, even introducing new ones, quickly spread globally and is said to have infected up to ten million computers in total (Porras, Saidi & Vinod, 2009). Over the course of the next few years, an international community of global actors, primarily industry actors and some law enforcement agencies, took an effort to take this botnet down (Conficker Working Group, 2012). Despite all endeavours, every time this group discovered a vulnerability in Conficker to take it down, a new variant was released fixing this flaw, rendering the take-down attempts futile (Porras et al., 2009). It is interesting to point out that, while some collateral damage[38] was caused, Conficker did not have any malicious payload and was not used for actions commonly seen in a criminally motivated case of botnet infection, such as stealing information or conducting attacks via the established botnet. Some speculate that the creators of the botnet endeavoured to test the level of resilience of the Conficker botnet against take-down attempts, together with studying the response of the international community and its effectiveness. Whether Operation Conficker was conducted by a State, organised cyber crime or another powerful non-State actor has not been (officially) discovered so far, but all these types of actors would have the necessary skills and financial resources to develop and launch a botnet of this level of sophistication and keep the international community engaged for more than a year.

3.2 'Use' of Hacktivists and Cyber Criminals as a (Deniable) Force

It should be mentioned that in theory there are possibilities to use proxies for actions many States might consider hostile acts, while others might come to a different conclusion. Theoretically, a State could consider taking advantage of cyber crime actors or hacktivist groups in the area of its interest to conduct cyber actions as their proxies or with their support. The following are some theories on reasons for such a use of proxies:

- Some hacktivist groups and organised cyber crime elements represent reasonably powerful non-State actors, capable of launching malicious actions on a scale that might even become a threat to national interests. A State might find itself in a position where it is not able to block these elements to a reasonable degree and, as such, accepts it, turning the situation to its advantage by using these elements to carry out a State mission, or using them as a source for recruitment, getting access to the intelligence collected by them, or acquiring technology relevant for cyber operations that was developed by them.
- It might happen that some cyber criminals and especially hacktivists share common goals with the State in which they are located. Such a State might understand the actions by these elements aimed at others as patriotic acts in support of the

[38] This damage was primarily a side effect resulting from the techniques used to establish a persistent foothold on the infected IT system.

nation's wellbeing and, as such, would be less critical towards them than it would be in cases of, e.g., common criminal acts.

- There are commonly known regions with an increased amount of cyber crime or hacktivist activities. This fact might encourage a State to consider using cyber crime elements located in a region not affiliated with the State as a proxy for its own interests. This might result in false accusations from, e.g., the media or the public with regards to the responsible actor behind the activity coming from the region in question.
- Finally, some States might tolerate hacktivists or cyber criminal elements to some extent, as they might exert some level of pressure on other parties such as non-State actors, which the State does not favour.[39] Or they might generate some level of digital nose, drawing others' attention away from cyber activities a State might want to conduct without being detected.

4. A Toolbox to Build Cyber Power

With the main actors in cyberspace and some possible reasons for using proxies introduced, it seems appropriate to consider four dimensions along which a State can build up its cyber power:

1. it can build up State-owned capabilities,
2. it can rely on the industry to deliver the needed capabilities in the form of services, or by contracting highly skilled individuals,
3. it can build upon and encourage volunteers to aid the State in times of need, and
4. in theory, it can use existing elements of cyber crime or hacktivism in its favour.

These dimensions, as illustrated in Figure 2 *infra*, are not exclusive. Different States are likely to engage along these four dimensions to a different extent, and more forms may evolve over time.

[39] It is, e.g., known that cyber criminals are trying to damage the operations of other cyber criminals, e.g., by stealing botnets from each other. One might argue that this behaviour results in less efficient cyber crime as a whole, as it is wasting resources cyber criminals would otherwise use to conduct malicious actions against their victims.

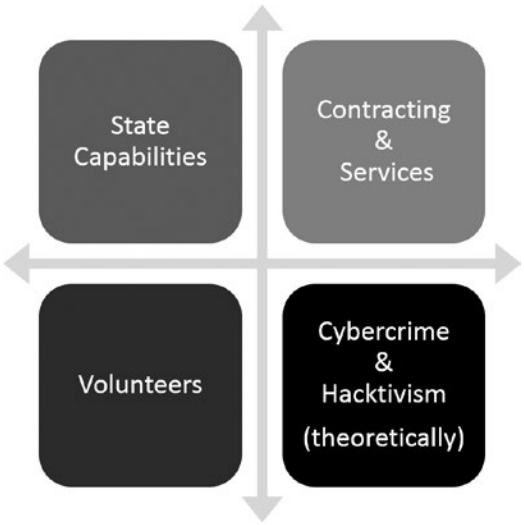

Figure 2. The four dimensions to build State cyber power.

In the following, the four archetypes depicted in the figure shall be introduced.

4.1 The 'Western Way': Capability Building and Contracting

For most Western States, the use of criminal elements is not an option. Instead they seek to mobilise and organise already existing national resources, primarily in the form of the industry providing ICT services, or national critical infrastructure providers. It is the latter who are likely to, in the end, suffer from the effects of cyber attacks against a State, if not suffering already,[40] and thus realise the need for better protection by, and cooperation with, the State.

States have developed different instruments to engage with the industry, such as voluntary cooperation programmes to facilitate sharing of information on threats or about attackers, best practice exchanges and consultation among industry and between industry and the State, and encouraging common anonymous reporting of security breaches by the private sector to an appropriate national authority. Sometimes private-public partnership initiatives are launched to share burdens, such as costs, to deliver public services by industry, or to initiate and encourage an activity which would lead to an industry-only programme later on.

40 One industry sector commonly regarded as part of national critical infrastructure is the banking sector, which has for some time already recognised the threat posed by cyber crime activities to their business.

In the context of the changing threat landscape, some States have established dedicated organisations, such as the UK with the Centre for Protection of National Infrastructure (2013), or integrated national responsibilities for critical information infrastructure protection into an already existing organisation, as carried out in the US with the Department of Homeland Security (2013). Others use already existing structures and increase their efforts, starting new, dedicated programmes such as the Federal Office for Information Security (2007) in Germany with its critical infrastructure programme implementation plan, including an ICT-related section 'UP KRITIS'. Similar programmes were initiated in the context of supranational organisations such as the European Union which, in the context of fighting cyber crime and with an increasing focus on the protection of critical infrastructure, launched a series of initiatives such as the EU Initiative on Critical Information Infrastructure Protection (European Commission, 2007, 2011) or the European Public-Private Partnership for Resilience program (European Commission, 2010). This plays a great part in establishing a powerful and resilient national cyber infrastructure for a State and, as such, enhances a State's level of cyber power.

The cooperation between industry and (Western) States for intrusive options has already been elaborated upon above and examples of the domains of law enforcement, espionage and military were presented. This illustrates that Western States are frequently turning to industry to buy specialised services if they are not able or willing to build the necessary capabilities themselves.

4.2 The (Better) Use of Volunteers

Despite the fact that the internet is the result of a former military research network to build a communication network able to operate even after major parts of it were destroyed, the internet as we know it today is the result of efforts of a largely volunteer community, forming an Internet Society (Klimburg, 2011).

One example is the Internet Engineering Task Force, a 'large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture' (Internet Engineering Task Force, 2013) with no formal membership, which develops and promotes most of the essential internet relevant technical standards. Another influential non-profit organisation is the Electronic Frontier Foundation, aiming 'to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today' (Electronic Frontier Foundation, 2013). In recent years, many more volunteer research and investigation organisations have formed, such as The US Cyber Consequences Unit dedicated to assessing 'strategic and economic consequences of possible cyber attacks and cyber-assisted physical attacks' (The US Cyber Consequences Unit, 2013). These investigators often focus on attacker attribution and feel little restraint in going public with their hypotheses and investigation results. In contrast to this, States have to consider the political impact of their accusations

and often are not willing to reveal the sources of their information because of national security concerns. It was, for example, Project Grey Goose (now part of Taia Global), a self-defined 'pure play Open Source Intelligence (OSINT) initiative' (Project Grey Goose, 2008) which collected and published reasonably dense situational evidence on the commonly assumed control by Russia over the cyber crime elements engaged in the 2008 Georgian-Russian cyber incident (Krebs, 2008). The Information Warfare Monitor Project, established in 2002 and closed last year (Information Warfare Monitor, 2012), became famous for its investigation of the cyber espionage network GhostNet, set up to spy on elements related to, or part of, the Tibetan government (Deibert, Manchanda, Rohozinski, Villeneuve & Walton, 2009), later publishing detailed information on 'a complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries (Bradbury & Rohozinski, 2010), putting a spotlight on some of the elements engaged in espionage and presumably located in China.

These examples highlight the presence of different, sometimes influential groups of volunteers, often acting independently from States in an effort to contribute in a way that they see as reasonable. Be it for publicity, or in an effort to support generally shared ideals between these individuals and particular political systems, the groups of investigators might prove increasingly powerful as an instrument against secretly State-sponsored cyber attacks (Klimburg, 2011). The challenge lies in how to take advantage of these volunteers from a national security perspective.

Estonia might be one of the few States which has succeeded in including a rather large part of its national non-State ICT actors into its national cyber security framework. Since its independence in 1991, Estonia has rapidly developed an ICT-friendly culture, willingly and quickly embracing new technologies and services made possible by the internet. As a result, Estonia developed a high level of dependence on information technology, becoming a vulnerable target for State-wide cyber attacks. At the time of the 2007 cyber attacks, initial State capabilities for cyber defence existed,[41] but the nationwide cyber attacks Estonia suffered (Ottis, 2008; Tikk et al., 2010) were ultimately mastered by the efforts of key industry players and volunteers, under the operational coordination of the Estonian Computer Emergency Response Team (CERT). As this system of actors proved successful, the community of volunteers gained official recognition and increased support, and felt validated for their efforts and the obvious need for them to help to defend their country against external threats. As a consequence, the Cyber Unit as part of the Estonian Defence League (formally known as the Cyber Defence League) was established, and Estonia introduced a legal and organisational framework to include volunteers in the State's national cyber security framework (Czosseck et al., 2011; Estonian Defence League, 2013).

41 The Estonian national Computer Emergency Response Team (CERT EE) was founded in 2006, but at this time had only a few staff members. Other dedicated agencies were not present.

As recently reported, other States are exploring a similar approach, such as Austria which, as one of the lessons identified from a national cyber security simulation game in June 2012, is openly considering to establish a 'volunteer cyber defence force'[42] to rely upon in cases of national crises caused by cyber attacks (DerStandard.at, 2013).

4.3 People's War and the Inclusion of Everyone

To some extent, hacktivists could be considered a special form of volunteers and, depending on the circumstances, some States might consider taking advantage of an already present hacktivist community. Hacktivists, if in favour of a State's goals, might be able to support a State in peacetime by offering intelligence and knowledge they might have acquired by their actions, or by offering their support in times of crisis. It may be China which stands out most in its approach on how to use these 'elements' for their good.

In public conviction, there is little doubt that a great amount of malicious activity is conducted by the hacking community in China. 'Of major cyber attacks publicly reported since 1999, two-thirds or more were probably directly associated with hackers in mainland China. Most media reports point out that these attacks are probably non-governmental in nature, but often say that the hacking is officially sponsored' (Klimburg, 2011). There are reports indicating[43] that China has enough influence on its hacking community to speak of State-controlled rather than State-sponsored activities.

A central concept in China's approach to defending its country against potential invaders is its strategy of *People's War*. The idea is that, by maintaining support by all citizens for, and by including them in, the defence of the country, a potential invader will be delayed and warned off by those applying guerrilla warfare strategies, giving the regular forces the opportunity to ultimately defeat the invader. In early 2000, the Central Military Commission increased its efforts to study this concept of People's War under conditions of 'informationisation' (Kanwal, 2009), and recent developments seem to prove that China is indeed successfully integrating this concept into its information warfare capabilities. China has developed decent military cyber strike capabilities under the adoption of its new Integrated Network Electronic Warfare Strategy which seeks to cripple adversary's C4ISR[44] systems at an early stage of a conflict (Krekel et al., 2009).

While this development might aim for preparing for future conflicts, it has two peacetime applications with regards to the use of hacktivist elements. In an effort to meet the intensive personnel requirements necessary to build up cyber warfare capabilities as

42 Freely translated from the Austrian term *Freiwillige Cyberwehr.*

43 In 2002, in anticipation of a reinflamed 'cyber war' between US and Chinese hacker groups as a sequential of the one conducted in 2001 (Delio, 2001), the US prepared for a new wave of cyber attacks by Chinese hackers. But it never happened, as 'the government of China asked them not to do that' (Hess, 2002).

44 Abbreviation for command, control, communications, computers, intelligence, surveillance and reconnaissance.

envisioned, China has reached out to its civilian sector, incorporating people with the skills needed. In this process, China has brought forth a complex system of actors of industry, academia, cyber crime and members of China's hacker community, with the lines between them blurred to the extent that single members seem to frequently switch roles (Klimburg, 2011).

Furthermore, it needs to be pointed out that, despite the fact that there is currently no sign of an emerging conflict between China and some other State and, as such, China should be considered as being in peacetime, the reality in cyberspace might look slightly different. Besides the fact that many cyber attacks are coming from the Chinese internet space, China is also suffering from a huge number of cyber attacks itself. As such, the efforts carried out by China in pursuit of its military aim to build information warfare capabilities, the concept of People's War in cyberspace might already have been tested on a daily basis.

4.4 Cyber Crime as a Way to Build Cyber Power

Similar to hacktivists and hacker communities, organised cyber crime elements could be seen as a source of skilled individuals for further governmental cyber activities.

Like other States, Russia is believed to be steadily developing State-owned cyber offensive capabilities. The first examples of these being successfully put into action reportedly go back to 1998 where, in a series of hacks, a large number of confidential files were exfiltrated from the US Department of Defense and the Department of Energy, as well as from the US National Aeronautics and Space Administration (NASA) and private organisations (Abreu, 2001). To further develop its cyber power and, at the same time, get the upper hand on cyber crime elements in the country, Russia is believed to have developed and is actively exploring new ways to take advantage of cyber crime elements within the country, while frequently denying any relationship with them.

There are many examples where Russian interests have been allegedly supported by elements of cyber crime without any official link to, or direct control by, the Russian government. In the case of the Estonia incident in 2007, Russian hacktivists inside and outside of Russia, as well as botnets said to be under the control of cyber crime elements, at some point joined forces in supporting Russian interests by conducting DDoS attacks against Estonian targets (Ottis, 2008). The same is believed to have happened in 2008 during the Russian-Georgian conflict, where cyber attacks were even coordinated with conventional military movements, indicating at least some decent level of control over the officially independent non-State actors. Some reports indicate even a direct attribution to Russia (greylogic, 2009). Furthermore, there are examples of cyber attacks against critical media and opposition parties prior to elections (Nazario, 2009). While many cases show pressing circumstantial evidence, indicating at least

some level of influence, or even control, by the Russian government, hard evidence is difficult to find or might not be there at all.

It gives the impression that Russia is indeed tolerating cyber crime to a certain degree, reflected in its limited or slow actions taken against cyber crime activities. At the time, and in the aftermath of the 2007 cyber attacks against Estonia, law enforcement cooperation requests by Estonia to Russian authorities, to identify attack sources in Russia, were not answered (Ottis, 2008). The above-mentioned RBN (see section 2.2), which supposedly was shut down by Russian authorities in 2007 after pressing international demands, seems still active in a more distributed network of organisations, with the head of RBN said to be protected by the highest political ranks in Russia (Klimburg, 2011).

Again, as in the example of China, cyber crime in Russia seems to be a potent source for recruiting talent. And, as with the services provided by specialised industry in Western States (and also in Russia itself), cyber crime offers a marketplace for products and services enabling or supporting 'customers' in their activities (Jarrod Rifkind, 2011).

5. Conclusion

While State action regarding the internet was, for a long time, primarily driven by economic considerations and the protection of personal data of citizens, the new century saw a rapid and significant change in priorities towards acknowledging the national dependency on information and communication technology. Nowadays, the protection of ICT systems supporting the critical infrastructure of a State from cyber attacks is a commonly seen priority for most States and, at the same time, is linked with a global 'arms race' to acquire and increase cyber power and, with it, the ability to project power by cyber means. But with an overwhelming majority of skilled ICT professionals capable of properly defending or penetrating ICT systems being non-State actors, States are left with the question how to get an edge against the industry, other States and actors in the competition for this talent. States also have to realise that, when it comes to questions of cyber power, many independent non-State actors exist who have acquired some significant amount of power themselves, leaving States with the choice to either coexist or deal with them. Activating slumbering or yet unconsidered national resources and incorporating them for the State's sake seems to be an area offering new opportunities.

The ways States approach this challenge may differ significantly and could include fostering volunteer actions by industry and civil society elements, the use of contractors and industry services, and the development of State-owned capabilities. Some States might even consider approaching cyber crime or hacktivist elements in this process. In the end, every State will have to develop a system of cyber power compatible with its legal, ethical and cultural norms.

However, all the presented examples of States having succeeded in establishing an relationship with non-State actors seem to have one common element, namely the willingness of the non-State actors to support their State's goals, be it for monetary or ideological reasons.

References

Abreu, E. (2001). Cyberattack Reveals Cracks in U.S. Defense | PCWorld. Retrieved September 29, 2013, from http://www.pcworld.com/article/49563/article.html

Billo, C., & Chang, W. (2004). Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States. Hanover: Institute for Security Technology Studies at Dartmouth College. Retrieved September 29, 2013, from http://www.ists.dartmouth.edu/projects/archives/cyber-warfare.html

black hat. (2013). BLACK HAT - ABOUT. Retrieved September 30, 2013, from https://www.blackhat.com/html/about.html

Bradbury, D., & Rohozinski, R. (2010). Shadows in the Cloud: Chinese Involvement in Advanced Persistent Threats. doi:10.1016/S1353-4858(10)70058-1

Centre for the Protection of National Infrastructure. (2013). Overview of CPNI. Retrieved September 29, 2013, from http://www.cpni.gov.uk/

Conficker Working Group. (2012). Conficker Working Group - Lessons Learned Document. Conficker Working Group. Retrieved September 29, 2013, from http://www.confickerworkinggroup.org/wiki/

Correll, S.-P. (2010a). 'Tis the Season of DDoS – WikiLeaks Edition | PandaLabs Blog. Retrieved February 09, 2011, from http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/

Correll, S.-P. (2010b). Operation: Payback Yielded 37 Days of Total Downtime. Pandalabs blog. Retrieved September 30, 2013, from http://pandalabs.pandasecurity.com/two-month-recap-on-operationpayback/

Council of Europe. (2001). Convention on Cybercrime. Retrieved January 01, 2012, from http://conventions.coe.int/treaty/en/treaties/html/185.htm

Council of Europe. (2013). Convention on Cybercrime - Status. Retrieved October 05, 2013, from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

Czosseck, C. (2012). An Evaluation of State-level Strategies against Botnets in the Context of Cyber Conflicts. Estonian Business School.

Czosseck, C., Ottis, R., & Talihärm, A. M. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. International Journal of Cyber Warfare and Terrorism (IJCWT), 1(1), pp. 24–34. Retrieved September 29, 2013, from www.ccdcoe.org

Deibert, R., Manchanda, A., Rohozinski, R., Villeneuve, N., & Walton, G. (2009). Tracking GhostNet: Investigating a Cyber Espionage Network. Information Warfare Monitor, Munk Centre, JR02-2009, March (Vol. 29, p. 53). Retrieved September 29, 2013, from http://www.nartv.org/mirror/ghostnet.pdf

Delio, M. (2001). It's (Cyber) War: China vs. U.S. www.wired.com. Retrieved September 29, 2013, from http://www.wired.com/politics/law/news/2001/04/43437?currentPage=all

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Networks and netwars: The future of terror, crime, and militancy, pp. 239–288.

DerStandard.at. (2013). Österreich überlegt Aufstellung einer 'Freiwilligen Cyberwehr.' derStandard.at. Retrieved October 07, 2013, from http://derstandard.at/1339639277027/Oesterreich-ueberlegt-Aufstellung-einer-Freiwilligen-Cyberwehr

EC-Council. (2013). EC-Council - About CEH v8. Retrieved September 30, 2013, from https://www.eccouncil.org/Certification/certified-ethical-hacker

Electronic Frontier Foundation. (2013). About EFF. Retrieved September 29, 2013, from https://www.eff.org/about

Emigh, J. (2010). RIM vs. India and Saudi Arabia: Let's Make a Deal on Encrypted Data. Brighthand. Retrieved September 29, 2013, from http://www.brighthand.com/default.asp?newsID=16910&news=BlackBerry+Blocked+India+Saudi+Arabia+Agreement+RIMM

Estonian Defence League. (2013). Estonian Defence League's Cyber Unit. Retrieved September 29, 2013, from http://www.kaitseliit.ee/en/cyber-unit

European Commission. (2007). Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC. Retrieved January 11, 2012, from http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=196418

European Commission. (2010). European Public-Private Partnership for resilience – EP3R. Retrieved January 16, 2012, from http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm

European Commission. (2011). Critical Information Infrastructure Protection. Retrieved January 16, 2012, from http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

Farivar, C. (2009). A Brief Examination of Media Coverage of Cyberattacks (2007 - Present). In C. Czosseck & K. Geers (Eds.), The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 182 – 188). Amsterdam: IOS Press. doi:10.3233/978-1-60750-060-5-182

FBI. (2013). Quick Facts. Federal Bureau of Investigation. Retrieved September 29, 2013, from http://www.fbi.gov/about-us/quick-facts

Federal Office for Information Security. (2007). BSI: CIP Implementation Plan. Retrieved September 29, 2013, from https://www.bsi.bund.de/EN/Topics/CriticalinfrastructuresImplementationPlan/implementationplan_node.html

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies, 8(1). Retrieved September 29, 2013, from http://epublications.bond.edu.au/cm/vol8/iss1/2/

Giles, K. (2011). 'Information Troops' – a Russian Cyber Command? In C. Czosseck, E. Tyugu, & T. C. Wingfield (Eds.), 2011 3rd International Conference on Cyber Conflicts. Tallinn: CCD COE Publications.

Giles, K. (2012). Russia's Public Stance on Cyberspace Issues. In C. Czosseck, K. Ziolkowski, & R. Ottis (Eds.), 2012 4th International Conference on Cyber Conflicts (pp. 63–75). Tallinn: CCD COE Publications.

Goncharov, M. (2012). Russian Underground 101. Trend Micro. Retrieved September 29, 2013, from http://www.trendmicro.co.nz/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Greenberg, A. (2012). Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits - Forbes. Forbes. Retrieved September 29, 2013, from http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

greylogic. (2009). Project Grey Goose Phase II Report: The evolving state of cyber warfare About Project Grey Goose.

Help Net Security. (2013). Nearly 200,000 new malware samples appear daily. Retrieved September 29, 2013, from http://www.net-security.org/malware_news.php?id=2521

Hess, P. (2002). China prevented repeat cyber attack on US - UPI.com. United Press International. Retrieved September 29, 2013, from http://www.upi.com/Business_News/Security-Industry/2002/10/29/China-prevented-repeat-cyber-attack-on-US/UPI-51011035913195/

Information Warfare Monitor. (2012). Information Warfare Monitor. infowar-monitor.net. Retrieved September 29, 2013, from http://www.infowar-monitor.net/

Internet Engineering Task Force. (2013). About the IETF. Retrieved September 29, 2013, from http://www.ietf.org/about/

Jarrod Rifkind. (2011). Cybercrime in Russia. Center for Strategic and International Studies. Retrieved September 30, 2013, from http://csis.org/blog/cybercrime-russia

Jellenc, E. (2012). Explaining Politico-Strategic Cyber Security: The Feasibility of Applying Arms Race Theory. In E. Filiol & R. Erra (Eds.), 11th European Conference on Information Warfare and Security (pp. 151–162). Laval.

Kanwal, G. (2009). China's Emerging Cyber War Doctrine. Journal of Defence Studies, 3(3), pp. 14–22. Retrieved from http://www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf

Keller, P. (2012). Cyberpower: Die Strategische Dimension. IT-Report ... -2012. IT-AmtBw, Cyber Defence, IT-Ausrüstung, IT-Lösungen, pp. 28 – 30.

Klimburg, A. (2011). Mobilising Cyber Power. Survival, 53(1), pp. 41–60. doi:10.1080/00396338.2011.555595

Kramer, F. D., Starr, S. H., & Kramer, F. D. (2009). Cyberpower and National Security (National Defense University) (p. 664). Potomac Books Inc. Retrieved September 29, 2013, from http://www.amazon.com/Cyberpower-National-Security-Defense-University/dp/1597974234

Krebs, B. (2008). Security Fix - Report: Russian Hacker Forums Fueled Georgia Cyber Attacks. The Washington Post. Retrieved September 29, 2013, from http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html

Krekel, B., Bakos, G., & Barnett, C. (2009). Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Northrop Grumman Corporation. Retrieved September 29, 2013, from http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved Report_16Oct2009.pdf

Landler, M., & Markoff, J. (2007, May 28). In Estonia, what may be the first war in cyberspace. The New York Times. Retrieved September 29, 2013, from http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html

Leder, F., Werner, T., & Martini, P. (2009). Proactive Botnet Countermeasures - An Offensive Approach. In C. Czosseck & K. Geers (Eds.), The Virtual Battlefield: Perspectives on Cyber Warfare. Amsterdam: IOS Press.

Leigh, D. (2010). How 250,000 US embassy cables were leaked | World news | The Guardian. The Guardian. Retrieved September 30, 2013, from http://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked

Levi, M. (2012). Measuring the Cost of Cybercrimes. ECRIM News Special Edition: Cybercrime and Privacy Issues, pp. 12–13.

Lewis, J. (2010). The Cyber War Has Not Begun. Center for Strategic and International Studies, (March), pp. 1–4. Retrieved September 29, 2013, from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Cyber+War+Has+Not+Begun#0

Manfreda, P. (2011). The Reasons for the Arab Spring. About.com. Retrieved September 30, 2013, from http://middleeast.about.com/od/humanrightsdemocracy/tp/The-Reasons-For-The-Arab-Spring.htm

Markoff, J., & Shanker, T. (2009). Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. NYTimes.com. Retrieved October 08, 2013, from http://www.nytimes.com/2009/08/02/us/politics/02cyber.html

Marson, S. (1997). A selective history of Internet technology and social work. Computers in Human Services, 14(2), pp. 35–49. Retrieved September 19, 2012, from http://www.tandfonline.com/doi/abs/10.1300/J407v14n02_03

Mc Cullagh, D. (2007). FBI turns to broad new wiretap method - CNET News. CNET News. Retrieved September 29, 2013, from http://news.cnet.com/FBI-turns-to-broad-new-wiretap-method/2100-7348_3-6154457.html

McLaughlin, V. (2012). Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind? Bachelor Thesis: University of Virginia.

Nazario, J. (2009). Politically Motivated Denial of Service Attacks. In C. Czosseck & K. Geers (Eds.), The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 163–181). Amsterdam: IOS Press. Retrieved September 29, 2013, from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Politically+Motivated+Denial+of+Service+Attacks#0

OPSWAT. (2012). Antivirus Market Analysis: December 2012 Software management and security solutions. Retrieved September 29, 2013, from http://www.opswat.com/about/media/reports/antivirus-december-2012

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In Proceedings of the 7th European Conference on Information Warfare (p. 163). Academic Conferences Limited.

Ottis, R. (2010). From Pitchforks to Laptops Volunteers in Cyber Conflicts. In C. Czosseck & K. Podins (Eds.), Conference on Cyber Conflict (pp. 97 – 108). Tallinn: CCD COE Publications. Retrieved September 29, 2013, from http://ccdcoe.org/229.html

Pelican, L. (2012). Peacetime Cyber-Espionage: A Dangerous but Necessary Game. CommLaw Conspectus, 20, 363–471. Retrieved from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=20+CommLaw+Conspectus+363&srctype=smi&srcid=3B15&key=a16b2163c9088fa4032c5d3515e69df5

Perry, W. (2007). Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. Occasional Papers Series, (28). Retrieved September 29, 2013, from http://www.offnews.info/downloads/perry_china_iw.pdf

Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. Information Security (p. 153). ENISA. Retrieved September 29, 2013, from http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

Poitras, L., & Gellman, B. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post. Retrieved September 29, 2013, from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Porras, P., Saidi, H., & Vinod, Y. (2009). An Analysis of Conficker. SRI International. Retrieved September 29, 2013, from http://mtc.sri.com/Conficker/

Pras, A., Sperotto, A., Moura, G., & Drago, I. (2010). Attacks by 'Anonymous' WikiLeaks Proponents not Anonymous. Enschede: University of Twente. Retrieved from http://doc.utwente.nl/75331/

Project Grey Goose. (2008). Project Grey Goose Phase I Report. Retrieved September 29, 2013, from http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report

Reuters. (2012, May 31). Cyber espionage on the rise, energy assets most vulnerable. The Economic Times. Retrieved July 09, 2012, from http://www.sustainabilityoutlook.in/news/cyber-espionage-rise-energy-assets-most-vulnerable

Russell, A. (2004, February 28). CIA plot led to huge blast in Siberian gas pipeline. The Telegraph. Washington. Retrieved September 29, 2013, from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html

Ryan, Y. (2011a). Tunisia's bitter cyberwar. Aljazeera. Retrieved September 30, 2013, from http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html

Ryan, Y. (2011b). Anonymous and the Arab uprisings. Aljazeera. Retrieved September 30, 2013, from http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html

Safire, W. (2004, February). The Farewell Dossier. The New York Times. Retrieved September 29, 2013, from http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html

ShadowServer. (2013). Shadowserver Foundation - Statistics on AV Products. Retrieved September 29, 2013, from https://www.shadowserver.org/wiki/pmwiki.php/AV/ImprovementBetweenInitialAndRetests

Starr, S. H., Kuehl, D., & Pudas, T. (2010). Perspectives on Building a Cyber Force Structure. In C. Czosseck & K. Podins (Eds.), Conference on Cyber Conflict (pp. 163 – 181). Tallinn: CCD COE Publications. Retrieved September 29, 2013, from http://ccdcoe.org/229.html

Symantec. (2011). Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually. Retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

The Daily Beast. (2009). The Evil (Cyber) Empire. The Daily Beast. Retrieved September 29, 2013, from http://www.thedailybeast.com/newsweek/2009/12/29/the-evil-cyber-empire.html

The Economist. (2007). A walk on the dark side. The Economist. Retrieved September 30, 2013, from http://www.economist.com/node/9723768

The U.S Cyber Consequences Unit. (2013). The U.S. Cyber Consequences Unit. Retrieved September 29, 2013, from http://www.usccu.us/

Tikk, E. (2009). Why Estonia Did NOT Invoke Article 5. Retrieved November 01, 2009, from http://www.enekentikk.net/2009/03/why-estonia-did-not-invoke-article-5.html

Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations (p. 130). Tallinn: CCD COE Publications.

U.S. Department of Homeland Security. (2013). Cybersecurity | Homeland Security. Retrieved September 29, 2013, from http://www.dhs.gov/topic/cybersecurity

UK Cabinet Office & Detica Ltd. (2011). The Cost of Cyber Crime. Retrieved August 01, 2012, from http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

UNIDIR. (2013). The Cyber Index - International Security Trends and Realities (p. 153). Retrieved September 29, 2013, from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Voß, O. (2011). Überwachungs-Software: Auf der Spur des Trojaners - Digitale Welt - Technologie - Wirtschaftswoche. Wirtschaftswoche. Retrieved September 29, 2013, from http://www.wiwo.de/technologie/digitale-welt/ueberwachungs-software-auf-der-spur-des-trojaners/5756462.html

Winter, M. (2013). NSA uses supercomputers to crack Web encryption, files show. USA Today. Retrieved September 29, 2013, from http://www.usatoday.com/story/news/nation/2013/09/05/nsa-snowden-encryption-cracked/2772721/

Mauno Pihelgas

Back-Tracing and Anonymity in Cyberspace

1. Introduction

This chapter focuses on tracing back malicious actors who are trying to remain anonymous in cyberspace. The aim is to describe possible ways in which they might be operating to avoid detection and association with their true identity. Additionally, different techniques will be discussed which could be used to identify and trace the origins of malicious actors.

Cyberspace is widely used for online governmental services, business transactions and personal communication on a daily basis. As a result, cyberspace is an attractive target for a wide range of malicious actors, whether they are corrupt insiders, foreign intelligence services or just curious computer enthusiasts experimenting with some new tools found on the internet.

Everybody who uses any online services (e.g., shopping, banking) – including, more importantly, administrators responsible for managing these essential systems – needs to be aware of the risks that are involved. Technology nowadays allows malicious actors to steal and transfer massive quantities of data while remaining relatively anonymous and hard to detect. The proliferation of anonymisation techniques and malicious software makes it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the risk of economic espionage, and the intelligence community judges that the use of such tools is already a greater threat than more traditional espionage methods [1]. Meanwhile, the amount of effort and resources required for back-tracing such attacks is increasing quickly. The security community is trying to deal with this problem, but they will need support when it comes to the legal aspects of their activities (e.g., whether or not it is legal to hack back to identify the attacker). In order to support such endeavours, the present chapter aims to provide a basic understanding of the technical aspects of computer networks, anonymisation techniques and back-tracing.

In the following, the basic terminology and technological background are explained first (2). Then, different techniques for remaining anonymous in online activities are introduced (3). Afterwards, possible ways of tracing the adversaries back to their origin are discussed (4), along with some considerations of the challenges, risks and obstacles involved in back-tracing. Finally, following a summary, some conclusions are drawn and the author's opinion is given as to how anonymity and back-tracing relate to attribution and misattribution (5).

2. General Background

This section introduces the basic concepts of cyberspace, in order to provide the reader with the necessary technical background to understand the following chapters. The aim is to offer general information without going into highly technical details of different protocols and technologies where it is not necessary. As in every specific field of study, it is first important to be familiar with some generic terms and expressions. Then a description will be given as to how computers communicate across the network and how can they be identified. Finally, the identification of different actors in cyberspace will be discussed.

2.1 Terminology

In the field of cyber security, many of the terms are not unambiguously defined. This chapter will be using some such terms and the following are the definitions and explanations which apply here:

Hacker – malicious actors or attackers are often called *hackers* by the general public, although, to avoid confusion, it is important to note that hacking purists refer to malicious ('black hat') hackers as *crackers* [2]. By this convention, a hacker is simply a computer security specialist who is committed to examining, developing and improving computer systems. These specialists devote their time to learning the ins and outs of systems upon which they are working. They are often called 'white hat' or 'ethical' hackers [3]. Although the distinction between the two types can sometimes be difficult, in this chapter we focus on the malicious (black hat) hackers.

Attack – in this chapter the term *attack* is considered to be any attempt to destroy, expose, alter, disable, steal, or gain unauthorised access to or make unauthorised use of anything that has value to an organisation [4]. In this sense, an attack does not have to succeed in order for it to be considered an attack. For instance, a person attempting to log in to someone else's account by guessing their user name and password could already be considered as an attacker. Another example would be that a hacker launches millions of bogus requests at a server, with the consequence of causing overload and higher latency[1] for other users of this server.

Event logs – stored datasets consisting of event messages. Event logs are often called simply *logs*. An event is a change in the state of the information technology (IT) system, with some predefined importance (e.g., a malicious network packet is sent to the web server). When an event occurs, the system could emit an event message that describes the event. For convenience, event messages are often called simply *events*. Event logging is a procedure of writing event messages to local or remote data storage [5].

1 Latency is the time delay between a request and response.

2.2 Identification Features of Devices on the Internet

Computers on the internet have many types of identification features that are common to all devices. Some of the more significant aspects that help to identify specific machines on the network (e.g., the internet) are discussed in this section. For example, every device (node) on the network must be assigned a unique Internet Protocol (IP) address to effectively communicate with other devices on this network.

An IP address is an identifier for a computer or other network device during an internet session. An IP data packet is the basic element of data transmission via the internet. It comprises a header (containing information on the source, destination, status and fragmentation of the transmitted data) and a payload (containing the transmitted data). At the very beginning of the internet, IP addresses were statically assigned to particular users (usually companies, organisations, universities and, rarely, to individuals). The assignment of IP addresses or IP address ranges is now regulated by the Internet Corporation for Assigned Names and Numbers (ICANN).[2] Since February 2005, ICANN has delegated this task to five Regional Internet Registries (RIRs), i.e., regional organisations assigning IP addresses. These are AfriNIC (Africa), APNIC (Asia and Pacific), ARIN (North America), LACNIC (Latin America and Caribbean Region) and RIPE NCC (Europe, Near East and Central Asia). Usually, an internet user receives a dynamic IP address from the pool of IP addresses at the disposal of an internet service provider (ISP), for that particular internet session only. After the internet session ends, the dynamic IP address is released and can be assigned to another user of the ISP. The so-called static IP addresses are mainly used by major corporations and other entities; they are also available to individuals for a specific fee.

As already mentioned, every device communicating on the network does have an IP address. In addition to regular desktop and laptop computers, nowadays many other devices, such as mobile phones, tablet computers, printers, and television sets are also capable of connecting to a network. In order to do so, they must have an IP address assigned to them. Currently, there are two versions of IP standards used side-by-side: IP version 4 (IPv4) and IP version 6 (IPv6).

2.2.1 IP Version 4 (IPv4)

At the time of the writing, IPv4 is still the most widely used networking protocol that has been around since the beginning of the 1980s. In technical terms, IPv4 uses 32-bit addresses, which means that over four billion (2^{32}) unique addresses can be composed

[2] ICANN, the Internet Corporation for Assigned Names and Numbers bears global responsibility for ensuring the stable and secure operation of the internet, as well as for coordinating the internet system of unique identifiers, i.e., for the assignment of IP address ranges, DNS root zone, and other internet protocol resources. ICANN is contracted by the US Department of Commerce to perform the functions of the Internet Assigned Numbers Authority (IANA), which was executing the above-mentioned tasks directly on behalf of the US Department of Commerce, and is now a department of ICANN [39].

using this standard. IPv4 addresses can be expressed in many different ways. The most common way of writing an IP address is the dotted decimal representation, which looks like this: *192.0.43.10*.[3]

Public IPv4 address space has been allocated by ICANN to various entities and registries all over the world (see the list of RIRs in section 2.2 above). Furthermore, it is important to note that there are some blocks (IP address ranges) which have been reserved for use in private networks and other specific purposes. For example, private IPv4 address space has been reserved for the following address ranges: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255 and 192.168.0.0 - 192.168.255.255 [6]. Any user may freely use any of the private addresses, although the user still needs to avoid assigning the same IP address to two or more different machines on the same network, because this would result in an IP address conflict and these machines would not be able to communicate properly on the network. To illustrate this, imagine two people with exactly the same first and last names living together in the same apartment: they would both have exactly the same address, so sending mail to one of them specifically would be impossible without using any additional identifiers.

As mentioned above, IPv4, which is currently the dominant networking protocol on the internet, provides approximately four billion IP addresses, which was considered to be sufficient in the early days of the internet but has been officially exhausted since February 2011, when all public primary address blocks had been allocated to different RIRs [6]. This does not mean that are no IPv4 addresses available; large allocated IP address spaces still contain smaller, unused blocks. Additionally, as mentioned above, there are also some IP address blocks that are reserved for use in private networks and these can be reused in every private network. For instance, a company can have hundreds or thousands of computers and only use one external (public address space) IP to connect to the internet. In this case the company's external network router[4] masquerades the private addresses on the network and all the requests to the internet seem to be originating from one particular IP.

2.2.2 IP Version 6 (IPv6)

The exhaustion of IPv4 address space has not come unexpectedly. The issue had already been addressed in the middle of the 1990s, when the Internet Assigned Numbers Authority (IANA) put together an IPv6 Working Group which was responsible for the specification and standardisation of IPv6 [7].

---

3 This IPv4 address corresponds to the domain name 'www.example.com'.

4 A router is a networking device that forwards data packets between two or more computer networks. Based on information from the packet headers, it directs traffic to the next network towards its ultimate destination. Nowadays, many small office and home routers are also designed to offer many other functions (modem, web server, firewall, etc.) in addition to just routing packets between networks.

IPv6 uses 128-bit addresses, which results in a significantly larger address space (2^{128} unique addresses). Similar to IPv4, there are some IP address blocks (ranges) that have been reserved for special or future usage. A common representation of IPv6 addresses is the hexadecimal format, which looks like this: *2001:0500:0088:0200:0000:0000:000 0:0010*[5] or *2001:500:88:200::10* when abbreviated. Unfortunately, IPv4 and IPv6 are not interoperable, so this has resulted in a complicated transition from IPv4 to IPv6. In many cases, this means that IPv4-only devices cannot directly communicate with IPv6-only devices. The first option is the use of tunnelling, where IPv6 packets are encapsulated in IPv4 packets and transmitted over old IPv4 infrastructure, but this only enables end-to-end connection between IPv6 hosts. A second option would be to use IP header and address translation between the IPv4 and IPv6 protocols to facilitate communications for different protocols. These two options are only meant as a temporary means to aid the transition from IPv4 to IPv6. Finally, there are dual-stack networks, which are able to operate IPv4 and IPv6 protocols in tandem; however, it may require significant investment to replace the current network infrastructure with such devices. IPv6 has slowly been making its way into common use and is becoming more popular every year. However, judging by current trends, it seems that IPv4 will still be around for many years to come [8].

2.2.3 Media Access Control Address

A Media Access Control address (MAC address) is a unique identifier assigned to all network devices by the manufacturer. It is also often referred to as *hardware* or *physical address*. The common representation of a MAC address is the hexadecimal format, which looks like this: *84-34-97-20-56-E5* or *84:34:97:20:56:E5*. The first three segments are unique to the manufacturer of the device and the last three segments are unique to the specific device interface. If a device has multiple network interfaces (e.g., wired and wireless), all of them have a unique MAC address. Although MAC addresses may look similar to IPv6 addresses, they are not to be confused with each other.

A MAC address is used for the communication of devices on one network segment. This means that the physical address of a computer inside a local area network is not communicated further from the gateway router to the internet. Externally, from the internet, only the MAC address of the gateway router's WAN[6] port can be identified by the ISP. Thus, when it comes to MAC addresses, the information is only relevant at a local or ISP level.

Furthermore, modern hardware usually allows the user to modify the MAC address willingly; this technique is called *MAC spoofing*. This can be used to mask the actual identity, or to intentionally fake the identity of some other device. For instance, some

5 This IPv6 address corresponds to the domain name 'www.example.com'.

6 WAN is the abbreviation for Wide Area Network.

ISPs only allow predetermined MAC addresses to connect to their network to prevent misuse on the client side. When a client connects a new computer or router, they would no longer be able to connect to the network and would have to contact the ISP to replace the MAC address. Instead, some users use MAC spoofing and modify the MAC address to be identical to the old device. However, this means that the old device cannot be used on the same network with the same MAC address, as this would result in a MAC address conflict.

2.2.4 Domain Name System

Domain Name System (DNS) is a naming system for resources connected to a network (e.g., the internet). It is used to translate agreed-upon system names (domain names) to IP addresses that are used to actually locate the resource on the network. DNS enables the use of easily memorable domain names instead of more complicated IP addresses. Consider the difficulty of remembering the different IPv4 or IPv6 addresses mentioned in previous chapters in order to visit *www.example.com* or any other website on the internet.

Domain names have a hierarchical structure that is separated by dots. In the example (www.example.com) above, *com* is the top-level domain and *example* is its subdomain (also called *vanity domain*[7]). Following this pattern, *www* is in turn a subdomain of *example.com*. Usually *www* refers to the main website of some domain, but this is not a fixed requirement. To clarify this a little further, take, for instance, some other domain names like *mail.google.com*, *es.wikipedia.com* or *support.apple.com*. These all have more elaborate names for their subdomain that takes the user directly to the website they are trying to reach.

DNS is an attractive target for attackers because users heavily rely on it for most operations on the internet. If attackers manage to insert falsified data into a DNS server, it is then called 'poisoned'. As a result, the server may start referring its users to a false IP address that the attackers have set up to serve malicious content. For example, if users type *www.example.com* into their web browsers, a request is then made to a DNS server to resolve this domain name to an IP address. That DNS server would normally respond with the correct IP address (93.184.216.119) of this website. However, if the DNS record is manipulated, the server would refer the user to another IP address (website) which the hackers control. If this website is made to look like the original *www.example.com,* users would probably not even notice that something is wrong. Now, imagine this happening to an online banking website where users would unknowingly enter their log

7 A vanity domain is a domain name that is specifically chosen by the registrants to portray their name, activity or any other combination that might attract users to visit or easily remember them. For example, the domain *youtu.be* is a shortened domain name that redirects the user to *www.youtube.com*.

in credentials: malicious actors controlling the website would receive the user names, passwords, etc.

2.2.5 WHOIS

WHOIS is a public query and response protocol that is used to query databases that hold information about internet resources, such as domain names and IP address allocations. The WHOIS protocol can be used to query an IP or domain name to determine the responsible company, relevant ISP information or point of contact (POC) for any problems regarding this address. The WHOIS utility is freely available on most operating systems and can even be used online as a web service [9].

If an IP address is found to be the source of suspicious traffic, it can be queried using the WHOIS protocol to identify the point of contact for this IP address. The response usually contains the information of the registrar and the registrant. However, because of privacy concerns, domain registrars often do not disclose all the information about their customers when third-party or command-line tools are used. Instead, the WHOIS information displays the registrar's contact information or a referral to a website, where another WHOIS query can be made to reveal more details (email addresses, phone numbers, etc.). This website verifies (e.g., by using a CAPTCHA[8]) that the information is requested by an actual human, not an automated computer script gathering POC information. It is important to note that, even on this website, the WHOIS request is still anonymous.

To give an arbitrary example, running a WHOIS enquiry for the domain of the Estonian Ministry of Foreign Affairs (MFA) *vm.ee* reveals that the domain registrar is RIKS.[9] It lists the name and phone number of the registrar. Additionally, the name of the registrant and two specific persons are listed as POC for this domain. However, as mentioned above, the command-line tools or other third-party WHOIS web refer to the web-based WHOIS service from the Estonian Internet Foundation (EIF) *www.internet.ee*. From the EIF website, the specific email addresses for different POCs are revealed.

A report from ICANN, the managing body for the WHOIS directory, recently stated that the WHOIS directory, which is currently anonymously available, should be shut down. Although it can be a useful tool when lawyers have sought to determine the identity of abusive registrants in domain disputes, ICANN has stressed that the DNS has become far more complex than it was when WHOIS was introduced 25 years ago. Some people in ICANN have even stated that WHOIS is broken and often inaccurate. Thus, they

8 CAPTCHA is an acronym for Completely Automated Public Turing test to tell Computers and Humans Apart. It uses a challenge (typically a distorted or complex image) where the user has to respond to the system and describe what is displayed in the image. The idea is that challenges like this are hard for computers to automatically solve.

9 RIKS stands for Riigi Infokommunikatsiooni Sihtasutus (in English: State Infocommunication Foundation).

have reached a decision that WHOIS, with its current design, should be abandoned and a new system introduced to address these issues. Registration data should be collected, validated and disclosed for permissible purposes only, with more sensitive data being accessible only to authenticated requestors that are held accountable for appropriate use of the information [10] [11].

2.3 Identification Features of Different Actors

There are many ways of identifying different actors operating in cyberspace, although it may not be as easy as one would imagine. It largely depends on the proficiency of the attacker and the amount of effort they have made to conceal their identity.

2.3.1 Proficiency of the Attacker

As already mentioned above, the proficiency of the attacker could be considered as one key aspect of the overall difficulty of detecting the origins of the attack. In short, well-experienced attackers would know how to organise professional attacks and hide their tracks. Based on proficiency and motivations (e.g., financial gain, damage to reputation), malicious actors could be divided into following categories [2]:

- 'Script kiddies' – this is a derogatory term for inexperienced computer enthusiasts who use malicious tools available online to attack networks and deface websites to gain fame.
- Black hat hackers – malicious hackers who break into different networks and computers. They are always trying to come up with new kinds of attacks and looking for vulnerabilities in the systems in order to gain access to them.
- Hacktivists – usually politically or religiously motivated hacker activists who target corporations and governments, trying to expose their illegal activities or simply exacting revenge for subjectively perceived wrongdoings.
- Criminal hacker groups – professional black hat hackers who are available for hire, e.g., by corporations to infiltrate a competitor's computer systems. They spy on and perform attacks to sabotage the competitor's business on behalf of their clients.
- State funded hacker groups – hackers who are enabled and funded by governments to spy on and target civilians, corporations and other governments. They are potentially hired to control cyberspace on behalf of their government.
- Cyber terrorists – usually motivated by religious and political beliefs, these hackers are attempting to spread fear and terror by claiming to disrupt critical infrastructure services, such as water supply, electricity and communication.

2.3.2 Information from the Media and the Internet

Hackers are often perceived as isolated individuals who prefer to act alone. However, analysis from 2011 [12], based on monitoring interactions in hacker forums, have shown that they are, in fact, quite social. Many of them are actively visiting online forums and chat rooms to communicate with other hackers. They could be seeking fame and glory amongst their peers for their achievements. Additional activities include sharing knowledge, exchanging tips, and trading tools and stolen data (e.g., user names and passwords, credit card data), etc.

Therefore, it can be inferred that monitoring these forums may provide security specialists with some warning about when and what kind of attacks are being organised. Moreover, after attacks have taken place, hackers could be bragging about their recent actions or selling stolen data. It should be noted that hackers use aliases or the name of their group instead of real names when posting any information on forums or chat rooms. However, this information could prove useful when tracking the actions of different hackers or groups. When the identity of one hacker is discovered, this could potentially reveal other previous attacks as well.

2.3.3 Language and Unique Style

Sometimes the origin or nationality of the attackers can be guessed by the language they have been using. Although most programming languages are implemented based on English, there are some elements inside program source code that can be named more or less freely by the author. Additionally, a well-written source code is usually supplemented by comments from the author. These are optional notes included to explain or improve later understanding of the code. If such elements are written in another language, this could possibly insinuate the native language of the author.

Thus, if a malicious program or code snippet was recovered after an attack, there might be some information that can point to the author of this program or code. For instance, there could be some comments or a unique reference to the author of the program. It can be helpful, even if it is just a nickname. Those nicknames could possibly be associated with claims of successful hacks which have been made to the media and on the internet.

2.3.4 Unique Tools and Techniques

Hackers often create and reuse automated tools and malware for gathering preliminary information about targeted systems: for instance, scanning for security vulnerabilities and gaining access to these hosts by means of some detected exploit. However, automated tools often leave patterns and signals that could potentially be detected when the same tool pattern is detected again. When these tools are acquired and analysed by malware specialists, some unique patterns or signatures could be discovered, which might reveal the type and nature of the analysed tool. Subsequently, new signatures

could be developed for intrusion detection systems and distributed to users. However, this is not always possible; some cleverly designed tools might not be unambiguously distinguishable from normal traffic patterns.

2.3.5 Action Patterns

Sometimes specific patterns are identified when it comes to the different attack stages of hackers and hacker groups. This topic will be discussed in more detail in a dedicated chapter in this volume.[10] However, it is important to note that attacks rarely take only a few hours, as is often seen in movies. Instead, attacks often take days, weeks or even months to plan and execute. Different stages of the attack are evened out across time to avoid detection. Although sometimes quick attacks can be successful, they will be more easily detected by any system defences, since they are more likely to cause anomalous system behaviour and network traffic. There is some theoretical reasoning behind this, e.g., when a hacker believes that the intrusion was detected (but is not yet blocked), the hacker might be trying to extract as much information or inflict as much damage as possible before security specialists are able to block access to the systems.

3. Anonymity

The term anonymity refers to remaining publicly unknown. In cyberspace, this can also be associated with remaining private and protecting the identity of an individual during online activity. Trying to stay anonymous online does not necessarily have to be associated with malicious activity: most people and companies have plenty of reasons to pay attention to the privacy and security of their online activity. Applying basic methods of privacy can even protect regular users from hacking attacks; for instance, it can be extremely helpful when using public wireless networks (e.g., at cafes, airports, etc.), where there can be many curious individuals locally eavesdropping on the network traffic.

3.1 Possible Uses for Anonymity

Many companies are already using a technique called virtual private networking (VPN) to keep their data private on the internet. For example, employees working from remote locations (e.g., home, cafe, abroad) have to use a company VPN service to connect to the company's resources. Furthermore, this technique is also used to connect branch offices in various locations to the central company resources over the internet without revealing sensitive company data at any intermediate point. More detailed explanations will be given *infra* (section 3.2).

---

10 See Markus Maybaum, 'Technical Methods, Techniques, Tools and Effects of Cyber Operations' in this volume.

Users often try to remain anonymous when they are engaging in private, political, malicious or criminal activities. For example, people could be searching the internet for some topics (e.g., medical, religious, etc.) with which they would not like to be associated. Another reason could be that some countries limit freedom of speech and forbid any unfavourable political activities, so the only way for insiders to tell the world what is actually happening is through anonymisation channels. Judging by some of the examples, there are plenty of ways that anonymity and privacy can be used for good reasons, such as:

- protecting private information (e.g., passwords, social security and credit card numbers);
- conducting business and commercial transactions;
- freedom of speech (in terms of political as well as non-political claims);
- freedom from detection, retribution and embarrassment;
- reporting illegal activity or misconduct (e.g., whistleblowing);
- law enforcement efforts in detecting online criminal activities (e.g., police anonymously observing chat rooms and forums for illegal activities).

When it comes to anonymity, there is a fine line between good and evil intent. Managing privacy on the internet is essential for malicious actors. Anonymity offers malicious actors the possibility of conducting illegal activities without the prospect of prosecution. Therefore, there are many negative aspects associated with anonymity, such as:

- spamming;
- phishing;
- denial of service (DoS) attacks;
- anonymous bribery;
- copyright infringement;
- harassment and threats;
- financial scams;
- disclosure of trade secrets;
- theft of other sensitive information.

3.2 Remaining Anonymous in Online Activities

There is no such thing as being completely anonymous on the internet, although there are several ways that reasonable privacy can be achieved using anonymisation techniques. Each technique has different levels of effectiveness and also potential drawbacks. A rule of thumb is that staying anonymous is a costly endeavour – not necessarily financially, but it definitely requires more effort from the user, and there is a trade-off with ease of use, connection latency and bandwidth [13] [14].

Hackers could be concealing their identity during attacks in different ways. One would be to try to destroy all evidence (e.g., log files) of the attack, so that it would be extremely difficult to analyse what had happened. The other would be to use a stolen identity (e.g., names, documents, images, etc.) in order to lead the investigation in a wrong direction. For instance, an identity could have been stolen by using the spying functions in malware mentioned *infra* (section 3.2.4).

Encryption and a well-considered use of personal information are of key importance in staying anonymous online. In the following subsections, several techniques which can be used or combined in the anonymisation process will be explained. In order to avoid confusion, it is important to note that the following figures and examples are based on the popular client-server model [15]. This means that the term *client* is used to refer to the party to a communication process that is requesting service from a *server* (service provider).

3.2.1 Proxy Servers

On a day-to-day basis, most users connect to different resources on the internet directly using their home or work internet connection, which means that the IP address assigned to them by their ISP is logged by the services they use or websites they visit. Proxy servers enable the users to hide their IP address by directing all specific type of traffic (e.g., web browsing) through another server; see Figure 1 below for an illustration as to how a proxy server works. Most modern web browsers can be configured to use proxy servers in similar fashion. The accessed host does not necessarily have to be a web server; proxies can be used for other services as well.

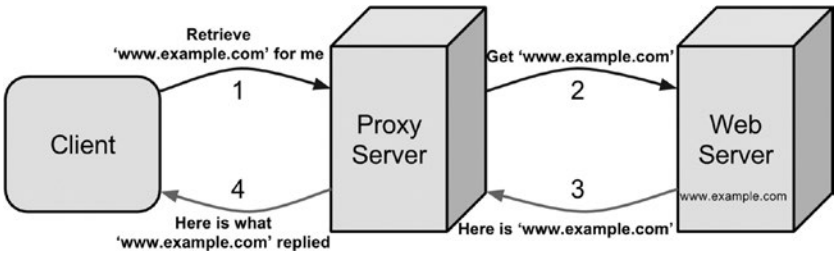

Figure 1. Example of a web proxy service; the client accesses the web server by relaying the request via a proxy server.

Proxy servers offer different levels of anonymity. According to HMA! Free Proxy List [16] the following levels of anonymity servers are available:

- no anonymity – the web server knows the client's IP and knows that a proxy is used. The proxy forwards the client's IP address to the web server;
- low anonymity – the web server does not know the client's IP, but it knows a proxy is being used;
- medium anonymity – the web server knows that the client is using a proxy, and thinks it knows its IP, but the IP used is not the client's. This is usually a proxy with multiple interfaces which shows its inbound interface's IP address to the web server, or
- high anonymity – the web server does not know the client's IP and has no direct proof of proxy usage (no references to a proxy connection in the request). If such hosts do not send additional header strings it may be considered as highly anonymous. However, such a host may very likely be a honeypot (i.e., 'too good to be true').[11]

Such proxies can be found and used for free (e.g., HMA! [16]), but those usually offer lower-speed and higher-latency connections. Many such service providers also offer a paid service with better access to good quality proxy services. Some ISPs offer their clients proxy servers as well, but it seems that they were used more often back in the day when internet connections were slower and less stable. Due to caching[12] features, the proxy servers were able to serve popular pages and content more quickly to the users. Otherwise each user had to download all the content from the original source, which put more load on the network; consuming valuable bandwidth and increasing overall latency.

Many companies still use proxies in their networks due to security reasons. For example, employees are only allowed to connect to the internet via a company proxy, which performs security checks on the traffic that passes through. The proxy could include anti-virus scans and block traffic based on blacklisting[13] or website reputation ratings.[14] This would enable the company to detect security incidents faster and protect their employees more efficiently.

11 A honeypot is a trap set to detect, deflect or, in some manner, counteract attempts at unauthorised use of information systems. Generally, it consists of a computer or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain valuable information or resources [37]. Honeypots can also be set up by scientists to gather valuable information about hackers' behaviour and tactics.

12 A cache is a fast data storage component that is used to serve future requests quicker.

13 A blacklist in this context is a list of IP addresses, domains or keywords that are not allowed to pass through the proxy.

14 Website reputation ratings are usually calculated by some algorithms based on user ratings or statistics reports from security tools. A site can be rated bad when it is spreading malware, spyware, spam or trying to exploit some vulnerability in the user's system.

3.2.2 Virtual Private Network Servers

Another good method of achieving privacy is tunnelling the entire network traffic to a server in another location before data is transmitted to the resource that the user is actually trying to access. By using VPN, all network traffic is encrypted between the start (*client*) and endpoint (*server*) of the tunnel. See Figure 2 below for an illustration of VPN service usage. The VPN server often acts as a proxy for either some internal network, or for forwarding requests back to the internet; the requests would seem to be originating from the VPN server's IP address.

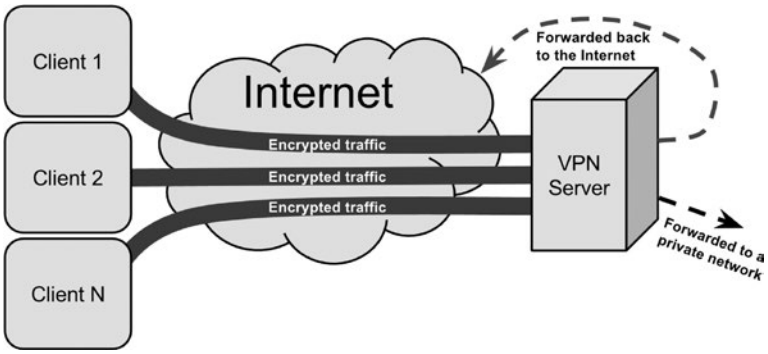

Figure 2. Basic example of VPN usage; clients connect to the VPN server through the internet.

There are different kinds of protocols by which VPN (tunnelling) connections can be configured; however, going into specific technical details would certainly exceed the scope of this chapter.

VPN is often used when employees need to connect to company networks from outside the office (home, abroad, etc.). This will enable them to work with internal company assets without exposing them directly to the internet (and potentially many malicious actors). Note that even the term *virtual private network* comes from virtually extending the private network to other remote locations across public networks (e.g., the internet). Companies with branches in multiple physical locations can use such tunnelling to enable direct communication between branches in different parts of the country and the core network of the company. For instance, a store's checkout terminals could be connected to the company's central database to keep track of inventory details (e.g., quantity and price). Using this method, the database services do not have to be exposed directly to the internet.

Connecting to a VPN can also be useful when public unsecure networks need to be used. Encryption of all data transmission will conceal the details of the online activity from any curious individuals that might be listening in on the network traffic. This

is especially important regarding data that is not encrypted in the first place (e.g., Hypertext Transfer Protocol, or HTTP traffic, unencrypted sending and receiving of email, etc.).

There are publicly available (usually paid) services for VPN available online [17]. It is important to note that the tunnelled traffic is decrypted at the tunnel endpoint and, from there on, any unencrypted data will be easily readable again. Therefore, the location and the security of the VPN endpoint are crucial to the privacy of the communication. The trustworthiness of a commercial VPN service provider has to be considered as well, since they are in a position to associate the network traffic with a specific user of their service.

3.2.3 Use of Anonymity Networks (Onion Routers)

There are special anonymity applications that enable the user to access the internet anonymously. They make use of multiple public or private proxy servers that relay encrypted data across several randomly chosen nodes on the anonymity network. This technique is more generally called onion routing. The name refers to an analogy of removing layers from an onion: multiple layers of encryption have been applied to the transmitted data, and each relay node decrypts (removes) the following layer until the original data is revealed and sent to the intended recipient. See Figure 3 below for an illustration of the onion routing process, using three randomly chosen nodes. Each node removes one layer of encryption to reveal the original data that is to be sent to the target host.

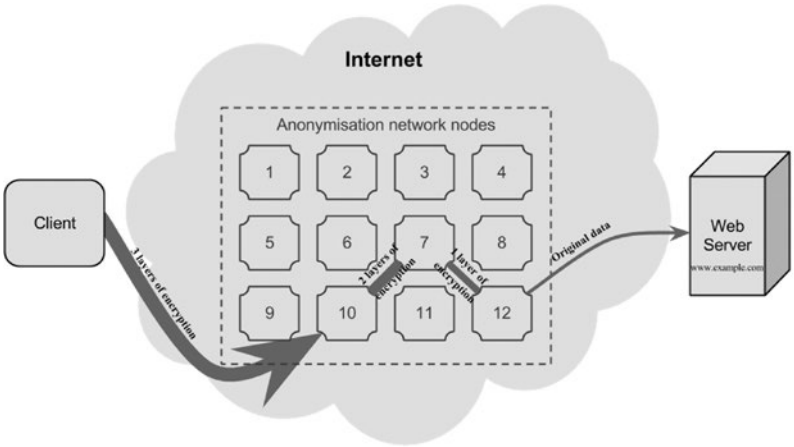

Figure 3. Example of a request to a web server through three random anonymisation network nodes.

One of the more popular anonymity applications used nowadays is Tor (originally short for The Onion Router). Due to its widespread popularity, some of the following

explanations will use Tor as an example. Tor was originally designed, implemented, and deployed by the United States (US) Naval Research Laboratory for the use of the US Navy, with the primary purpose of protecting government communications [18].

The group behind Tor claims that it is used every day by a variety of individuals and entities, including the military, journalists, law enforcement officers, and activists. It is also reported that a branch of the US Navy and law enforcement institutions have used Tor to gather intelligence and keep websites under surveillance without leaving government IP addresses in the web server's log files [18]. The Tor Project [19] offers the reader many examples of Tor usage that can be useful in understanding the possibilities of this anonymisation network. Tor is free software that helps to reduce the risks of sophisticated traffic analysis by distributing online transactions over several steps on the internet, so no intermediary point can associate the source of the traffic with its destination. The idea is to use a twisty, hard-to-follow route in order to obfuscate the track, periodically erasing the user's 'footprints'. Instead of taking a direct route from source to destination, data packets select a random path through several (at least three) relays that cover the user's tracks so that no observer at any single point can have knowledge of both where the data came from and where it is going [18]. Similarly to the VPN services described before, the last node of the onion route will see the data as it was compiled by the original sender in order to forward it to the destination of the traffic. This means that, even when using onion routing, it is important not to disclose any private information that is communicated unencrypted to the destination. Ideally, even the traffic entering and exiting the anonymity networks (between the source and destination) should be encrypted.

Tor even offers a specifically designed, live Linux operating system called Tails (short for The Amnesic Incognito Live System) to use its anonymisation network even more securely and privately. This system can be used to start a computer straight from a DVD or USB memory stick and, therefore, it will leave no trace on the computer's hard drive [20].

Tor relay nodes are hosted by volunteers all around the world. There is a general rule that the wider the variety of people using Tor, the more anonymous it will be, because network traffic will be obfuscated and made harder to track by other users of the network.

3.2.4 Malware Infected Zombie Computers

Attackers could remain anonymous by assuming the identity of someone else. Malware-infected computers could be used to perform malicious actions on behalf of the actors that are controlling the malware. Additionally, malware enables the hackers to steal data from infected computers and spy on the activity of their users. One way to achieved this is by using Remote Access Tools (also known as Remote Access Trojans, or RATs) to provide a 'backdoor' into the systems. Computers are often accidentally infected by

opening malicious email attachments, downloaded files, etc. These files are usually presented as legitimate programs to trick the users into installing them without being aware of their devices becoming infected. After infecting the system, most likely the computer will become a member of a larger botnet.[15]

There are many RATs available with different levels of functionality. More capable ones will enable the hackers to perform virtually the same tasks as accessing the computer physically. Below are some of the possible activities that the hacker could perform on a victim's computer when in control of a RAT:

- spy on the user:
  - log keystrokes (e.g., steal user names, passwords and other personal information);
  - capture screen images;
  - capture audio from the microphone;
  - capture images or video from the webcam;
  - read email;
  - access files on the hard disk.
- manipulate data and system activity:
  - access the internet (e.g., send email or perform attacks on other systems);
  - create, modify and delete files;
  - install or uninstall software;
  - start or close applications;
  - shut down or restart the computer.

Some of the more interesting functions are as follows. A hacker could be accessing the internet from the infected system as if the owner of the computer was doing it; this could involve sending spam or infected emails to everyone in the owner's address book. Additionally, the hackers could abuse the information (names, dates, credit card numbers, user names, passwords, etc.) that they were able to steal by logging keystrokes or accessing files on the computer. Furthermore, this will allow them to stage malicious activities in such a way that the other person would be held responsible (e.g., by planting incriminating evidence to lead the tracing and investigation in a certain direction).

3.2.5 Concealing Personal Information

Last but not least, concealing personal information is the most basic technique that is meant to serve as a general recommendation that applies to all previous points, rather

[15] Botnet is short for robot network. It is a network of malware infected personal computers. A botnet can consist of tens of thousands or even hundreds of thousands of zombie computers [35]. A botnet is controlled by a command-and-control (C&C) server, which can send the zombie computers (bots) instructions to initiate or cease an attack against some predetermined targets.

than a specific technical method. When users are trying to remain anonymous online, they should always consider what kind of data they reveal about themselves. Even if they are using complex anonymisation techniques (proxies, Tor, etc.), it might all be in vain if they use their real name and information on a website (especially if the website does not use encryption, i.e., so-called HTTPS protocol[16]) or log into their social media accounts (e.g., Facebook, Twitter) during the same internet session. Sometimes this can happen even unintentionally, for instance if the web browser remembers data from previous sessions and uses this data automatically (e.g., logs in the user automatically after returning to a website).

The most effective solution to avoid such problems would be to use a bootable live operating system CD, DVD or USB flash drive (e.g., the system called Tails mentioned in section 3.2.3). Instructions for creating and using these live operating systems are available for many Linux/Unix operating system distributions [21]. These systems are used to start up (boot) the computer from a separate media (e.g., CD, DVD, USB), rather than the computer's hard disk. In most cases, they do not write anything to the hard disk so there is no history of the current (or previous) internet session. It is important to consider that the network connections of the computer can still be traced (e.g., by the ISP). Therefore, using a separate internet connection is recommended. Furthermore, as discussed in section 2.2.3, the MAC address of the network interface could be used to identify a computer. Thus, in order to avoid that, the MAC address should be changed before connecting the live operating system to the network and then reverted back to the original before restarting the machine from the hard disk again.

Another simpler, but potentially less effective, solution would be to turn on the In-Private (Incognito) Browsing mode on the web browser. Most web browsers nowadays have this functionality built in and available for all users. By using this method, the browser will not use or save any history past the current session. In their default configuration, browsers often continue the previous authenticated session, if it is still valid. For instance, the browser will log the user on without asking for login credentials, because it still has a valid session with that website.

To give an example of this, web browsers usually save *cookies* when visiting different websites. Cookies are data that are used by websites to identify returning users and restore any preferences they might have set during their previous visits. Usually this is a desired feature, because users do not wish to set their preferences again every time they visit a website. However, there can be an issue depending on how and what kind of data the website will store in the cookie. Data from the cookie could be used by the site owner, who receives this data upon every visit to the website. For example, a

16 HTTPS, or Hypertext Transfer Protocol Secure, is an application protocol for hypermedia information systems which works on top of SSL/TLS (Secure Sockets Layer/Transport Layer Security) cryptographic protocols, thus adding security capabilities to standard HTTP communications. HTTP is the base foundation for the World Wide Web (WWW).

discovery regarding how Facebook handles cookies was made in 2011: when a user has logged on to Facebook and logs out afterwards, the cookie on the computer will preserve its association with the user; thus, when visiting websites that have embedded the Facebook social plugin, the cookie data will give Facebook the ability to associate the visit to a particular webpage to a specific user, even if the user was logged out of Facebook. Facebook has commented that this is a security measure to detect spamming, phishing or other hacking attempts, which seems plausible. However, any further use of the data acquired with this method cannot be verified by the users [22].

To reiterate, these methods should be considered even when using any of the more advanced anonymisation techniques. This will prevent the computer from automatically sending out any saved data from previous internet sessions. There are many technical aspects that need to be considered when trying to remain anonymous; making a mistake in just one of them could potentially allow any activity of the system to be associated with the user's identity.

3.3 Challenges, Risks and Obstacles

As with most technologies, there are usually some ways in which anonymisation channels can be misused or attacked. Actors trying to stay anonymous during their online activity must be aware that there are numerous individuals with various ways and means which can pose a risk to their anonymity and privacy.

As mentioned above, the exit nodes of the anonymity networks and other proxies could possibly see the contents of the network traffic if it is not using secure end-to-end encryption. Intelligence agencies, scientists and possibly other curious individuals have been known to set up fake or malicious proxy nodes (honeypot nodes) that, in addition to forwarding network traffic, also examine the contents of the packets and gather valuable data [23]. If the proxy is otherwise working properly, the users have no way of knowing whether their private data is being analysed or not. However, this is more of a random attack against the anonymity network, because the exit node cannot directly control which nodes are connecting to it.

Some sites may limit the activities that Tor users are authorised to perform. For instance, Wikipedia has, by default, disabled the ability to edit articles for users who are accessing the site from Tor networks. There is a possibility of acquiring an exemption for a specific IP address to enable access from countries that censor Wikipedia. The approval for an exemption has to be acquired individually on a per-user basis, so the users would have to prove their good intentions before they are allowed to edit articles. However, it can be difficult to remain anonymous during this verification process [24].

Anonymisation techniques might be vulnerable to traffic confirmation attack. When an entity such as an ISP or some intelligence agency has the ability to monitor network usage in large networks (e.g., at the global, continental or country level), they may

use traffic timing analysis to correlate which hosts are actually communicating with each other, even when some anonymisation channels are used to relay this traffic. For example, when the initiating client and destination server are situated in the same monitored network, based on transmission timings and size, the ISP can correlate that these two hosts are indeed communicating with each other. Although this requires a good overview of the network and the use of advanced correlation techniques, it is technically possible to make such deductions [25] [26].

To illustrate this last point, Figure 3 in section 3.2.3 serves as an example. Assuming there is a server hosting illegal content and a law enforcement agency would like the ISP to identify clients who are accessing this resource. However, some clients were using anonymisation networks to avoid accessing the server directly. A traffic confirmation attack tries to identify situations where every time a particular client initiates a request, an incoming request to the server from some anonymisation network exit node follows shortly. It should be noted that the ISP can see traffic entering the anonymisation network (first step) and, just milliseconds later, exiting the network (last step). Although the traffic characteristics change when going through the anonymisation network, the timing and the pattern of the requests and responses is likely to give a fairly accurate result in confirming that the client and the server are indeed communicating. Although there is some risk in such tracking on a global scale, in 2004, the group behind Tor judged the risk to be small enough that for the moment it is not feasible to develop countermeasures to mitigate this risk [25] [26]. It is simply something for users to bear in mind when using various anonymisation channels.

4. Back-Tracing

This section will introduce the basic facts, concepts and processes related to back-tracing (also spelled ‘backtracking’) hackers who are performing attacks on computer systems. In terms of cyber security, back-tracing is the process of tracing the actions and steps taken to identify the originating source of communication. Or, more simplistically explained, to go back over the route by which one has come. When an attack has been discovered, an assessment of available data should be conducted as soon as possible. Security specialists must carry out an evaluation of information to determine the nature and objectives of the attack in order to make trustworthy and timely decisions to deter the attack.

Judging by the attack methods, as well as number and distribution of incoming attack sources, it should be possible to assess whether the operation is conducted by a single individual or a group of hackers working together. Sometimes the attacks are distributed in a way that no single source can be determined, for example, when multiple hackers initiate attacks simultaneously against a number of targets. Furthermore, the attackers could be in charge of a botnet of malware-infected zombie computers. In any case, incoming requests could be originating from different countries all around the world.

4.1 Gathering Relevant Information from the Attacks

When it comes to network and cyber-related issues, back-tracing is usually performed when a security incident has occurred, or some suspicious activity on the systems has been detected. Before back-tracing can take place, security specialists need to determine what has happened in the first place. They must gather information about the attack from the affected systems, which usually involves analysing the log files the systems have produced, hopefully revealing what was carried out, and which IP addresses were behind it. Furthermore, inspecting changes made to the system configuration and carrying out an analysis of the event log files that the affected machines have created are necessary. This could be a lengthy and complex process because hackers try and hide their activity from plain sight. Moreover, systems can sometimes create large amounts of log messages which can slow down the process of finding relevant information (e.g., the attacker's IP address). Nevertheless, by analysing this information, security specialists can potentially assess the intention and scale of the attack. Furthermore, with the extracted IP addresses they can also determine the network nodes that are performing the attack, but it is important to bear in mind that this could likely be an exit node of some anonymity network.

If the attacks are recurring or still ongoing, there is the possibility of monitoring the attackers' activity more effectively in real time. This will offer several ways of actually learning more about the attackers; potentially revealing their intentions along with their identity. Additionally, the defending security specialists could set up honeypots to lure the hackers into a trap. In some ways this would turn the table on the hackers and make them the research subject. If successful, specialists would be able to gather useful information about the behaviour, proficiency and intentions of the intruders. With this data, the security of the actual production systems could be adapted and improved to prevent further unauthorised access.

4.2 Tracing Attackers

After an IP address (or several) has been extracted from logs or obtained by any other means, the next step would be to find out as much information about it as possible. This subsection describes some of the processes and tools involved in tracing the actual network routes hackers have taken to access a resource. It is important to note in advance that all of the described tools or methods are not guaranteed to produce any useful results. This is simply one possible set of resources and techniques that could be used in such situations. It is still necessary for the security specialist to analyse the results and make educated assessments on a case-by-case basis.

4.2.1 The Traceroute Tool

One of the most basic tools for tracing back attackers is called traceroute.[17] It is a tool which, as the name says, traces the route network packets take from the machine running the tool to the target host. It was briefly explained in section 2.2 that data on the network is transmitted in packets and each packet has a header and a payload. Traceroute uses cleverly crafted network packet headers to elicit a response (i.e., a reply back to the host running the traceroute) from intermediary routers. Ideally this should reveal all routers between the source (i.e., the host running traceroute) and the target. However, due to the different configuration of network devices, traceroute sometimes fails to discover an accurate topology of the network. This is because specific protocols are often blocked, prioritised or routed differently from others. In order to help alleviate this issue, the traceroute tool enables the operator to select between different protocols (TCP, UDP or ICMP)[18] for gathering information about the examined routes.

```
traceroute to www.example.com (93.184.216.119), 30 hops max, 60 byte packets
 1  [redacted]
 2  [redacted]
 3  [redacted]
 4  kjj-bb3-xe-1-1-0-0.ee.estpak.ee (194.126.123.99)  2.676 ms
 5  tln-b3-link.telia.net (62.115.34.133)  2.534 ms
 6  s-bb3-link.telia.net (213.155.131.222)  12.761 ms
 7  kbn-bb1-link.telia.net (80.91.246.107)  21.831 ms
 8  hbg-bb1-link.telia.net (213.155.134.199)  27.999 ms
 9  ffm-bb1-link.telia.net (213.155.135.136)  39.706 ms
10  prs-bb1-link.telia.net (213.155.132.156)  46.602 ms
11  nyk-b2-link.telia.net (213.155.130.28)  108.963 ms
12  93.184.216.119 (93.184.216.119)  109.779 ms
```

Figure 4. Example of a traceroute output.

An output of the traceroute tool (see example in Figure 4 above) might not seem helpful at first, but it can prove useful for specialists, and for reporting malicious activity to the ISPs, who will have a better overview of the network nodes involved in the reported activity. When examining the output of the tool, it can be seen that, by default, traceroute combines the node's DNS name, IP address and response time for each hop along the route. Note that, in Figure 4, the first three rows have been blurred out due to the author's privacy concerns.

17 Traceroute is a tool that is freely available on most operating systems. It determines the path taken by packets to a destination. The tool utilises the IP protocol's time to live (TTL) field and attempts to elicit a response from each gateway along the path to the host [38].

18 Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Messaging Protocol (ICMP) are common network protocols used for communication and administrative purposes on the internet.

4.2.2 Location of the IP Address

Security specialists would most likely try to determine the best available location for the IP address. The traceroute tool will reveal the hosts between the source and the target. The device preceding the target host is most likely the gateway belonging to the ISP.

In addition to traceroute, there are other ways in which the location of the IP address, or at least the owner of the IP address, can be determined. For example, the WHOIS database sometimes also reveals the address of the registrant, but this does not necessarily have to be the physical location of the network device. Most often it is the official address of the registrant.

Moreover, approximate location (e.g., city) of the device can be assessed by using geolocation services available online. For instance, an online service called *MaxMind* was found to be the most accurate according to a series of tests conducted by Addy Incorporated [27]. Geolocation services utilise proprietary databases of addresses based on internet traffic flow and website registrations [28]. It is important to note that these services do not guarantee an accurate result.

4.2.3 Determination of the Point of Contact

As mentioned above, an individual or entity responsible for an IP address can be determined by using the WHOIS protocol. The WHOIS protocol often lists the contact information for abuse notifications in case any malicious activity has originated from the IP address. This would be the first point of contact in most cases. As stated before, it is important to remember that the host appearing as an attack source can also be the exit node of the anonymisation network, or a computer which was compromised by malware. The owner of this IP address might not be directly responsible or even aware of the misuse. In any case, the POC for the IP address should be contacted to request information about the incident.

Depending on the information gathered from the POC and their computer system, it could become evident that the steps in previous sections (tracerouting, determining the location and POC) have to be repeated to determine the same information about the next step towards the actual source of the communication. It could take several iterations before the original source is reached. For example, after contacting the owner of the VPN service or proxy server to acquire and analyse the logs regarding the attack, it is likely to be necessary to repeat the tracing process to reveal the next step in the route to the origin of the attack.

4.2.4 Enticing the Intruders into Revealing Their Identities

If none of the tools and techniques above provide any meaningful results, and if the attacks still are recurring, then there is the possibility of luring the hackers into revealing more details about their identity by using a cleverly designed trap.

A trap could be set by using special pieces of data called honeytokens.[19] Whereas honeypots are resources (computers, systems or applications) that no legitimate user is supposed to be accessing, honeytokens are more specifically bits of valuable information that no one is supposed to be using; except the hackers who are to fall into this trap. For example, honeytokens could take the form of credit card information, account login credentials, computer files or some other forged, but seemingly highly valuable, information (trade secrets, classified data, etc.).

When the information from a honeytoken is abused by anyone, it should trigger an alarm to the security specialist and start detailed logging on the system to gather as much data as possible about the user of the honeytoken. Alternatively, the honeytoken information seems so valuable that the hacker just has to take action and do something with the data (e.g., log into an account, post something on a forum). With any luck the user of the honeytoken will reveal some form of additional information (e.g., another IP address or POC) that can be used for further investigation into the attacks.

Furthermore, security specialists could set up data leak detection mechanisms that would scan all outgoing network traffic, and monitor for specific codes, words, honeytokens and other predefined data structures. This could potentially detect both insiders and intruders extracting information from the company network. Although use of encryption could bypass more basic systems, real-life incidents have proven these mechanisms to be useful, for instance, in the case of a security manager tracing a leaked client list back to a recently resigned sales representative [29].

To illustrate this point about honeytokens a little further, a book called *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* by Clifford Stoll [30] describes the real-life efforts of a computer administrator (Stoll himself). He had to trace a hacker who had, on multiple occasions, gained unauthorised access to the Lawrence Berkeley National Laboratory computer systems. It took the author ten months of tracing, investigating and cooperating with various authorities in the United States and Europe to finally reveal the identity of the hacker behind the intrusion. Although the technology and systems described in the book are a bit outdated, it still offers the reader a good insight into the efforts required to trace a hacker.

---

[19] Honeytokens are a smaller subset of honeypots. More specifically, honeytokens are data that are stored in way that no one should be accessing them. Therefore, any interaction with a honeytoken most likely represents unauthorised or malicious activity. Honeytokens are cleverly crafted credible pieces of information that can be closely monitored when they are used [30].

It is worth mentioning that Stoll already used honeytokens in the middle of 1980s, but the term *honeytoken* was not actually used before 2003 [31]. Stoll planted fictitious material that would catch the hacker's attention by matching some of his search phrases (e.g., 'stealth' and 'nuclear'). This material kept the hacker on the line until his connection was traced back to the actual source.

4.3 Challenges, Risks and Obstacles

The following subsections elaborate some of the risks and challenges regarding back-tracing. Additionally, some forewarnings and general suggestions will be provided for consideration.

4.3.1 Feasibility of Back-Tracing

One aspect to consider is the feasibility of tracing the attackers. When the cost of dedicating resources to track down leads exceeds the benefit of catching the hackers, it might be wiser to invest those resources into securing the computer systems to mitigate the risk of other potential incidents.

Sometimes there might not be any feasible way to determine the route back to the source. This is, for example, the case if the tracing leads to an anonymisation network which is, by its very name, designed to be anonymous. These systems are built in a way so that they do not log long-term information about past communications. By using some of the weaknesses of anonymisation networks described in section 3.3, it might be possible to alter the anonymisation node to log this kind of information for future traffic, but of course it is not possible to acquire logs that were not created in the first place. Furthermore, since relay nodes are chosen randomly, there is actually little to no chance of catching the same hacker again.

Alternatively, an attack from a great number of different sources could indicate that the attacker has hired, or is in control of, a botnet. This could mean that the attack could be originating from thousands or tens of thousands of IP addresses all across the world. In case of a botnet attack, the owners of the infected computers will probably not be aware that their computers are used by others to conduct cyber attacks. It would not be feasible to try and track down the owners of all those computers. Instead, the person who ordered the attack or is in control of the botnet should be identified, but the Command-and-Control[20] (C&C) server is not directly identifiable from the perspective of the victim of the attack. However, the C&C server could possibly be determined by analysing

[20] A Command-and-Control (C&C) server is the system which controls a botnet of malware-infected zombie computers. A C&C server can send the members of the botnet (*bots*) instructions to initiate a set of actions or just remotely control the computers. For example, they can send instructions to initiate or cease an attack against some predetermined targets.

some of the zombie computers in the botnet. After identifying the C&C servers, the individuals controlling it could possibly be held responsible. Law enforcement and intelligence agencies and other institutions are constantly putting a great amount of effort into taking down botnets and their leaders [32].

Finally, it could also happen that the owner of a VPN or proxy service is just not willing to cooperate or provide any information. It could very well be the backbone of their business; protecting the privacy of their customers. In such cases the proper course of action would probably be to consider legal remedies and discuss the way ahead with law enforcement agencies. This could lead to lengthy and expensive court hearings that might not be worth the potential gain.

The harsh reality about back-tracing is that usually, even with a lot of effort put into tracking the adversaries, the actual names of the hackers will not be discovered by technical means. In many cases, back-tracing will only reveal that the attack came from an anonymisation network. It might also reveal the name of the ISP or company whose internet connection was used. However, ISPs typically release information about their customers only under court orders. This is why lawyers have to work with security specialists to gather as much relevant information as possible in order to be able to put together a strong case against the attackers.

Finally, if there is a considerable amount of proof that the identified IP address actually belongs to the hacker, it might not be wise to directly contact the suspect. This would give the perpetrator time to destroy any incriminating evidence that may be stored on their systems. For instance, erasing the hard drives of the computer could be done in a matter of seconds with the use of a *degausser,* a device that generates a strong magnetic field to cause irreversible damage to magnetic media types (such as hard drives, floppy disks, audio and video cassettes, etc.).

4.3.2 Recovering From an Attack

After an attack, system administrators, and even more importantly, management personnel would like to see the systems up and running again. Nowadays, when many systems are interconnected and rely on each other, uptime is as important as never before. However, quickly restoring system configurations, defaced websites, etc., can lead to loss of valuable data in terms of identifying the attacker. This can happen by restoring virtual machine images or replacing data from a previous backup. Therefore, it is important to bear in mind that the attacked machine should not be wiped to restore it, because deeper analysis of the data could be required.

4.3.3 Log Authenticity

Log authenticity has to be verified before making any conclusions. By default, most devices and operating systems log their events locally on the system itself. However,

this might not be secure in terms of information assurance. During an attack, the intruder will probably try to delete or modify the logs to avoid the possibility of logs leading back to him or her.

1. Central logging should be set up on the systems. With this configuration, all new logs are sent to a central log server as they happen. If the central logging is properly configured, tampering with the logs on the local machine will not affect the logs already collected on the central logging server.
2. Logging over the network should take place using secure, encrypted communication. This prevents eavesdropping and interception of the log contents.
3. Data authentication methods could be used to verify the authenticity of log files. For instance, a company called Guardtime is offering a service to timestamp and digitally sign all electronic and online transaction logs as they are created and stored: 'With these capabilities, organizations obtain and securely maintain the required forensic proof to solidify legal stances against intentional and unintentional insider attacks as well as external breaches, and other transactional-oriented fraud' [33].

5. Summary and Conclusions

This chapter has outlined the technical background of identifying various devices and malicious actors on the internet. This technical background serves as a prerequisite for understanding the main part of the work, which gives an overview of anonymisation and back-tracing techniques with some relevant illustrations. Definitions and explanations of various protocols and tools that are used to identify computers on the network have been offered. An overview of identification features (e.g., methods, aliases and level of proficiency) of hackers was also provided. Potential challenges, risks and obstacles for both anonymisation and back-tracing have been discussed and finally, some common problems related to attribution and misattribution in the context of back-tracing were outlined.

With regard to anonymisation, it was pointed out that anonymisation techniques are used for both good and malicious reasons. There is no basis for stating that being anonymous because of privacy concerns would be a disreputable activity: there are many valid reasons (e.g., protecting one's private information, conducting sensitive business transactions, preserving freedom of speech, reporting misconduct, carrying out covert law enforcement operations) for wanting to remain private and anonymous during online activity. Unfortunately, anonymity offers malicious actors the possibility of conducting illegal activities (e.g., theft of information, arranging cyber attacks) without the prospect of prosecution. When such malicious actors attack computer systems, it is necessary to find out as much information as possible about the attack and the attacker. This would require security specialists to analyse system log files and

decide on a further course of action. If the attacks are recurring, it might be possible to direct the attacker into a honeypot, or set up honeytokens for the attacker to find, so that the hacker would accidentally reveal his or her identity. Nevertheless, often it is still necessary to trace the network route back to the source to attribute the attacks to someone. Unfortunately, the reality is that back-tracing can be a difficult task that sometimes does not result in any clarity in terms of identifying the attackers.

With the evolution of different anonymity techniques, the difficulty of attribution is one of the primary challenges in reducing the overall insecurity originating from cyberspace and in tracing specific malicious actors. Accurate attribution is required to respond to cyber incidents in both the operational and legal terms.

Misattribution is a contrariwise problem, where an attack is made to appear to have originated from another source (incriminating someone else). In addition to slowing down correct attribution, this can result in risky situations where the blame is attributed to an innocent individual, organisation or country. Consequences can vary from conflicts and mistrust between parties to embarrassing incidents becoming public.

In the author's opinion, there is a need to emphasise the difficulty of back-tracing. It might seem that all the tools and methods are pretty straightforward with their results and outputs, but this may not be the case. There is a significant amount of effort required to track malicious actors, especially when dealing with more proficient adversaries. Even then, there is often a need for educated guessing when it comes to deciding which actions to take in terms of reaching the origins of the attacks.

Despite all the efforts, sometimes it is not possible to trace the attacks back to the source. For example, if the adversary does not make any silly mistakes and is skilfully using different anonymisation techniques, it might not be feasible to dedicate an unpredictable amount of resources to tracing this attacker. Instead, it may be wiser to invest these resources into improving security in order to mitigate the risk of any future attacks.

References

[1] Office of the National Counterintelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace,' October 2011. [Online]. Available: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. [Accessed 3 September 2013].

[2] R. Siciliano, 'Seven Types of Hacker Motivations,' Infosec Island, 25 March 2011. [Online]. Available: http://www.infosecisland.com/blogview/12659-Seven-Types-of-Hacker-Motivations.html. [Accessed 12 August 2013].

[3] Techopedia, 'White Hat Hacker,' [Online]. Available: http://www.techopedia.com/definition/10349/white-hat-hacker. [Accessed 12 August 2013].

[4] International Organization for Standardization, 'Information technology — Security techniques — Information security management systems — Overview and vocabulary,' 1 May 2009. [Online]. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip. [Accessed 24 July 2013].

[5] R. Vaarandi, Cyber Defense Monitoring Solutions Course: Event logs and syslog, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013.

[6] Internet Assigned Numbers Authority (IANA), 'IANA IPv4 Address Space Registry,' 20 May 2013. [Online]. Available: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml. [Accessed 18 June 2013].

[7] Internet Engineering Task Force (IETF), 'IP Version 6 Working Group,' [Online]. Available: http://datatracker.ietf.org/wg/ipv6/charter/. [Accessed 18 June 2013].

[8] Internet Society, 'World IPv6 Launch,' [Online]. Available: http://www.worldipv6launch.org/. [Accessed 18 June 2013].

[9] Internet Assigned Numbers Authority (IANA), 'IANA WHOIS Service,' [Online]. Available: http://www.iana.org/whois. [Accessed 15 July 2013].

[10] New Legal Review, 'ICANN earmarks domains record WhoIs for the scrapheap,' CPA Global, 12 July 2013. [Online]. Available: http://www.cpaglobal.com/newlegalreview/5558/icann_earmarks_domains_record_. [Accessed 30 September 2013].

[11] Expert Working Group on gTLD Directory Services, 'Initial Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service,' 24 June 2013. [Online]. Available: https://www.icann.org/en/groups/other/gtld-directory-services/initial-report-24jun13-en.pdf. [Accessed 30 September 2013].

[12] Imperva, 'Hacker Intelligence Summary Report – Monitoring Hacker Forums,' October 2011. [Online]. Available: http://www.imperva.com/docs/HII_Monitoring_Hacker_Forums.pdf. [Accessed 11 September 2013].

[13] R. Unger, 'Anonymity on the Internet,' [Online]. Available: http://www.cs.virginia.edu/crab/anonymity.ppt. [Accessed 26 August 2013].

[14] D. Prindle, 'How to Stay Anonymous Online,' Digital Trends, 16 May 2013. [Online]. Available: http://www.digitaltrends.com/computing/how-to-be-anonymous-online/. [Accessed 26 August 2013].

[15] B. Mitchell, 'Introduction to Client Server Networks,' About.com, [Online]. Available: http://compnetworking.about.com/od/basicnetworkingfaqs/a/client-server.htm. [Accessed 30 September 2013].

[16] Hide My Ass!, 'Free Proxy List,' Privax LTD, [Online]. Available: http://www.hidemyass.com/proxy-list/. [Accessed 2 September 2013].

[17] P. Gil, 'The Best VPN Service Providers, 2013,' About.com, [Online]. Available: http://netforbeginners.about.com/od/readerpicks/tp/The-Best-VPN-Service-Providers.htm. [Accessed 4 October 2013].

[18] Tor Project, 'Overview,' [Online]. Available: https://www.torproject.org/about/overview.html.en. [Accessed 28 August 2013].

[19] Tor Project, 'Who uses Tor?,' [Online]. Available: https://www.torproject.org/about/torusers.html.en. [Accessed 16 September 2013].

[20] Tor Project, 'Tails - Privacy for anyone anywhere,' [Online]. Available: https://tails.boum.org/. [Accessed 16 September 2013].

[21] N. Brand, 'The LiveCD List,' [Online]. Available: http://livecdlist.com/. [Accessed 30 September 2013].

[22] G. McMillan, 'Facebook Cookies Work Even If You're Logged Out (for Your Own Good),' Time, 26 September 2011. [Online]. Available: http://techland.time.com/2011/09/26/facebook-cookies-work-even-if-youre-logged-out-for-your-own-good/. [Accessed 27 August 2013].

[23] P. Gray, 'The hack of the year,' The Sidney Morning Herald, 13 November 2007. [Online]. Available: http://www.smh.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html?page=fullpage#contentSwap1. [Accessed 16 September 2013].

[24] Wikipedia, 'Advice to users using Tor,' [Online]. Available: http://en.wikipedia.org/wiki/Wikipedia:Advice_to_users_using_Tor. [Accessed 16 September 2013].

[25] R. Dingledine, N. Mathewson and P. Syverson, 'Tor: The Second-Generation Onion Router,' 18 May 2004. [Online]. Available: https://svn.torproject.org/svn/projects/design-paper/tor-design.html#subsec:threat-model. [Accessed 17 September 2013].

[26] The Tor Blog, 'One cell is enough to break Tor's anonymity,' arma, 19 February 2009. [Online]. Available: https://blog.torproject.org/blog/one-cell-enough. [Accessed 17 September 2013].

[27] Addy, Inc, 'IP Geolocation Services Showdown,' 18 October 2012. [Online]. Available: http://blog.addy.co/post/33835058393/ip-geolocation-services-showdown. [Accessed 30 September 2013].

[28] B. Mitchell, 'Does IP Address Location (Geolocation) Really Work?,' About.com, [Online]. Available: http://compnetworking.about.com/od/traceipaddresses/f/ip_location.htm. [Accessed 3 September 2013].

[29] M. Thurman, 'Security Manager's Journal: The sales rep and the honey tokens,' Computerworld Inc, 16 July 2012. [Online]. Available: http://www.computerworld.com/s/article/9229078/Security_Manager_s_Journal_The_sales_rep_and_the_honey_tokens. [Accessed 18 September 2013].

[30] C. Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, New York: Doubleday, 1989.

[31] L. Spitzner, 'Honeytokens: The Other Honeypot,' 2 November 2010. [Online]. Available: http://www.symantec.com/connect/articles/honeytokens-other-honeypot. [Accessed 18 September 2013].

[32] M. J. Schwartz, 'Microsoft, FBI Trumpet Citadel Botnet Takedowns,' InformationWeek, 6 June 2013. [Online]. Available: http://www.informationweek.com/security/attacks/microsoft-fbi-trumpet-citadel-botnet-tak/240156171. [Accessed 15 September 2013].

[33] Guardtime, 'KSI for Cloud Service Providers,' [Online]. Available: http://www.guardtime.com/solutions/for-cloud/#CSP_Logs. [Accessed 3 September 2013].

[34] Canadian Internet Registration Authority (CIRA), 'WHOIS Backgrounder,' 2013. [Online]. Available: http://www.cira.ca/utility-pages/WHOIS-Backgrounder/. [Accessed 11 September 2013].

[35] xyberShield, Inc, 'A Unique Approach Based on Understanding Hacker Behavior,' [Online]. Available: https://www.xybershield.com/Resources/HackerInsights.aspx. [Accessed 11 September 2013].

[36] McAfee, Inc., 'McAfee Threat Glossary,' [Online]. Available: http://www.mcafee.com/us/threat-center/resources/threat-glossary.aspx. [Accessed 15 September 2013].

[37] Hide My Ass!, 'VPN Service - Encrypt your internet connection,' Privax LTD, [Online]. Available: http://www.hidemyass.com/vpn/. [Accessed 15 September 2013].

[38] Defense Technical Information Center (DTIC) , 'Joint Publication 3-13.4 - Military Deception,' 26 January 2013. [Online]. Available: http://info.publicintelligence.net/JCS-MILDEC.pdf. [Accessed 16 September 2013].

[39] Linux man page, 'traceroute(8),' die.net, [Online]. Available: http://linux.die.net/man/8/traceroute. [Accessed 18 September 2013].

[40] Internet Corporation For Assigned Names and Numbers (ICANN), 'Welcome to ICANN!,' [Online]. Available: http://www.icann.org/en/about/welcome. [Accessed 30 September 2013].

Emin Çalışkan & Raimo Peterson

Technical Defence Methods, Tools, Techniques and Effects

1. Introduction

Cyber defence, as a very broad term, incorporates an endless number of subtopics. This chapter gives a simple overview of the main technical methods and techniques related to cyber defence for a non-technical audience. The chapter does not try to give a complete picture of all the possible subtopics of cyber defence; rather, a selection of the topics has been made by the authors after consulting the main target audience of this book – political and legal advisors. The aim of this chapter is to cover the selected technical topics in a simple way which is understandable to a non-technical audience. Most of this chapter explains the basic technical aspects of cyber defence as 'absolute truth' without further discussion. However, for some topics, there are on-going technical discussions wherein even technical experts do not have a common understanding. So the overall intent of this chapter is to give some technical background which is beneficial to those who are dealing with the political and legal aspects of cyber defence.

2. Information Security Objectives

Looking at information security[1] from a technical perspective, main information security objectives that an organisation is trying to achieve needs to be understood. Theoretically, it is possible to define one generic objective, stating that the overall target of information security activities is to secure information systems adequately. At the technical level, there is a need to specify what 'adequately secure' means.

Most commonly, cyber defence objectives are broken down into confidentiality, integrity and availability (CIA or the CIA-triad). There are several national and international information security standards available with similar breakdowns of information security. The definitions below are taken from the most referred to international standard ISO/IEC 27001:2013 [1]:

- confidentiality – the property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
- integrity – the property of protecting the accuracy and completeness of assets;
- availability – the property of being accessible and usable upon demand by an authorized entity.

[1] This chapter uses the terms 'information security' and 'cyber defence' interchangeably. However CIA based international standards are typically more 'information security' centric and for this reason in this section the term 'information security' is used predominantly.

In some scenarios, there may be a need to define even more specific security objectives like authenticity, accountability, non-repudiation, privacy, reliability and others. CIA-based models consider all these additional objectives as a subset of confidentiality, integrity or availability. For example, authenticity and non-repudiation can be considered to be a subset of integrity, privacy can be seen as a subset of confidentiality and reliability can be seen as a subset of availability.

Each organisation has usually implemented a set of information security controls which help to achieve the targets of one or more security objectives. For example, access control and data encryption are security controls which help to achieve the agreed targets of confidentiality. At the same time, these security controls can also improve integrity, but reduce availability. Therefore, first the security requirements are analysed and after that specific sets of security controls are developed, which helps to achieve the security objectives in the most cost-effective way. The corresponding methodology is defined by organisational Information Security Management System (ISMS) and will be covered in section 7.3.

3. ISO-OSI Model and Encapsulation

Before jumping to more technical topics like Internet Protocol version 6 and deep packet inspection, we need to cover the layering model of the internet communication and the encapsulation-decapsulation process through the layers. The International Organization for Standardization (ISO) Open Systems Interconnection (OSI) model [2] (usually called 'ISO-OSI model') was defined decades ago and has not lost its importance even today. It helps to break down network communication into understandable pieces, which is beneficial for developing applications[2] and communication protocols.[3] It also helps in troubleshooting, and is useful for training purposes.

The ISO-OSI layering model defines seven abstraction layers. These layers are named in the ISO standard, starting from Layer 1 as: Physical, Data Link, Network, Transport, Session, Presentation and Application layer. In this chapter, for simplicity, we are combining three upper layers (Application, Presentation and Session) into one and will refer to it as the application layer. The four lower layers (Transport, Network, Data Link and Physical) take care of the transport of the application data over the network (either Local Area Network (LAN) or internet). The application layer is where the applications work and produce data to be sent over the network to their communication peers using application protocols, like Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), telnet (a terminal emulation protocol that enables an internet user to log on to a

2 An application, in computer science, is a piece of software such as a web browser, chat client, word processor or any other which is developed to perform specific tasks.

3 Communication protocol defines message formats and rules, so both parties using the same protocol will interpret the message in the same way. It is similar to the human language – both parties speaking the same language will understand the message in the same way.

remote computer or network) and hundreds of others. Each layer fulfils its functionality by means of layer specific protocols. In order to communicate, the other party must have the same protocol implemented. In other words, both parties must understand the protocol, which is comparable to language in human communication.

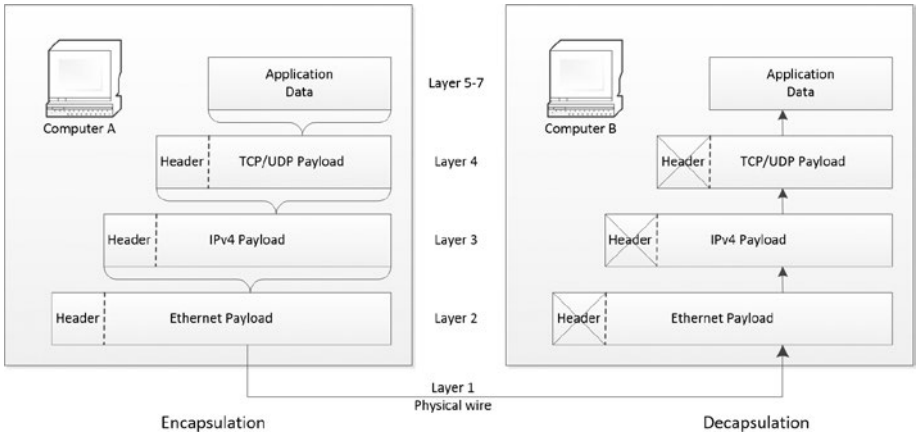

Figure 1. Data encapsulation-decapsulation in ISO-OSI Model.

In order to facilitate communication over the network, the lower layers add additional headers and trailers to the application data (see Figure 1). Trailers are not shown in Figure 1 for the sake of simplicity. The headers and trailers of different layers add useful information for routing the data via the internet, for establishing communication channels, for error detection and correction and for other functional purposes of each layer. For example, a layer 3 header contains source and destination Internet Protocol (IP) addresses,[4] and layer 2 headers contain source and destination Media Access Control (MAC) addresses[5] among other data. The process of adding headers and trailers by lower layers to the upper layers' data is called encapsulation and the process of ripping off the headers and trailers at the receiving station is called decapsulation. The exact format of the header and the packet itself is defined by the protocol of the corresponding layer.

4 An 'IP address is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication', see http://en.wikipedia.org/wiki/IP_address.

5 A MAC address is the address in layer 2 header. Local Area Network (LAN) switches are using MAC address for forwarding Ethernet frames. It has only local importance and is not sent over the internet. Each device connected to the network has a unique MAC address.

The protocols shown in Figure 1 (TCP[6], UDP[7], IPv4[8] and Ethernet[9]) are just the most common examples of the protocols of a given layer. Internet Protocol version 4 (IPv4) is one, and it is the most commonly used layer 3 protocol. Several years ago Internetwork Packet Exchange (IPX) was a popular layer 3 protocol and now Internet Protocol version 6 (IPv6, see details in section 5.4) is emerging.

If the packet travels through the network, some networking devices on the way look only to the layer 2 header for the MAC address, while others decapsulate the incoming bit stream up to layer 3 looking for the IP address. For example LAN switches (see Figure 2) connecting the computers in a local network segment are looking only for the layer 2 headers and forward the frames to other switches based on a MAC address taken from the layer 2 header.

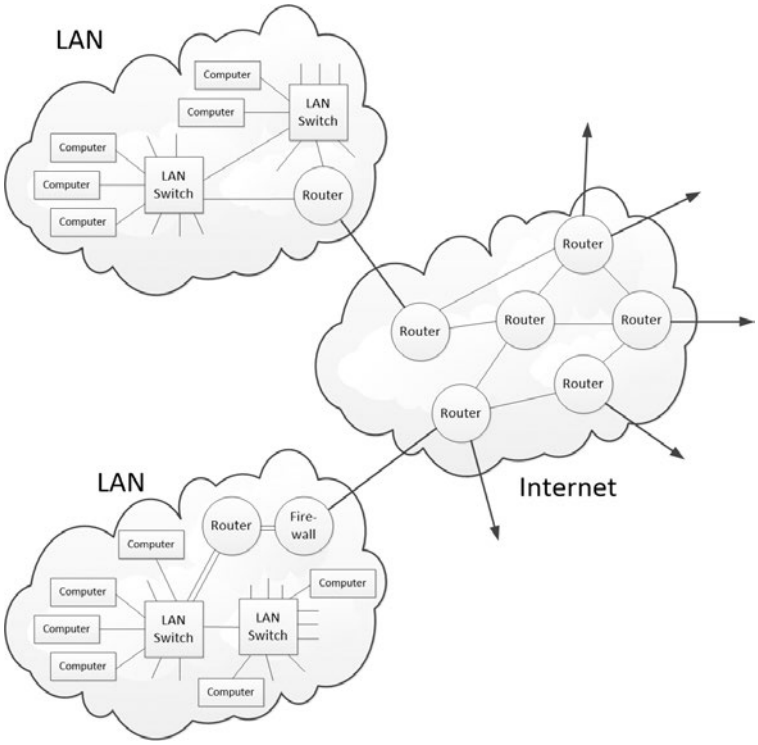

Figure 2. Deployment of switches and routers in networks.

6 TCP – Transmission Control Protocol; major layer 4 protocol which is responsible for assembling otherwise loose packets into connections. Often IP protocol together with TCP is referred as TCP/IP protocol.

7 UDP – User Datagram Protocol; layer 4 protocol for connectionless communication.

8 IPv4 – Internet Protocol version 4; most commonly used layer 3 protocol that will be replaced by IPv6 in future.

9 Ethernet is a layer 2 protocol used in local networks; LAN switches are forwarding the Ethernet frames based on MAC addresses.

Routers connecting the internet are looking for the destination IP address from the layer 3 header of the incoming packet (see Figure 3). Routers do not need anything from the upper layer data to provide their main functionality. Therefore routers do not waste resources on decapsulation of the higher layer data.

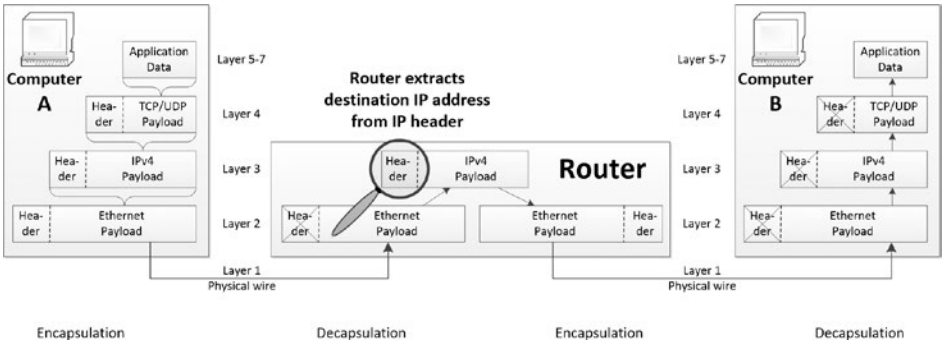

Figure 3. Router operation.

Decapsulation of the data up to the application layer can be beneficial in some network nodes. This allows analysing of the data and searching for malicious patterns. It also enables searching for data from specific users and searching for specific keywords, phrases or patterns. It is possible to make automatic blocking, prioritizing, forwarding, recording or network optimisation decisions based on the predefined criteria. This is called Deep Packet Inspection (DPI; see details in section 4.2.5).

Applications and application layer protocols may have vulnerabilities which can be exploited via application layer attacks. If malicious data targeting application layer vulnerabilities is sent over the internet, it is encapsulated and hidden by several layers. Therefore ordinary network devices (switches and routers) are usually not able to determine if the data they are forwarding is malicious or not. At the same time attacks are not only targeting vulnerabilities in the application layer: vulnerabilities exist in each layer.

4. Security Applications and Devices

In this section, various security applications and devices, as well as new trends in cyber security such as honeypot systems, will be discussed. Switches, routers and other networking devices and applications like Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and firewalls will be introduced briefly. After this introduction, honeypot systems will be elaborated on in detail to explain how they can be useful to collect additional information related to cyber attackers.

4.1 Network Devices

Although one may think there can only be end nodes, such as a server and a client computer, during internet communication, there are also other devices between those end nodes. Switches and routers, as we are introducing below, are the two main components of such devices (see Figure 2 above).

In general, security devices can be implemented in two different ways. Usually, any new functionality is implemented by a software package running on a general-purpose computing-hardware. As time goes by and the functionality gets mature enough, and there is enough need in the market, an Application Specific Integrated Circuit (ASIC) is developed. The reason for developing ASICs is about much higher performance of ASIC and also the cost factor. Several years ago switches working on layer 2 were hardware devices and routers running on layer 3 were software devices. Nowadays both can be realised by hardware ASICs and therefore the performance of the higher-layer devices has improved tremendously.

4.1.1 Switches and Routers

Classical switches operating on layer 2 of the ISO-OSI model are multi-port networking devices interconnecting systems in local networks. It means that they are forwarding frames based on the information in the layer 2 header, mainly based on the MAC address which has local importance. Switches do not look into the IP addresses in the layer 3 header of the packet and therefore they are not able to perform internet routing. Classical switches are very fast and reliable layer 2 devices.

Routers are more advanced networking devices than switches. Classical routers are devices working on layer 3 which means that the packets are forwarded based on the information in the layer 3 header, mainly the IP addresses which have global importance. Routers interconnect networks using routing tables. Routing tables are lists to guide which network packet should be forwarded to which network segment. Routers are located at gateways, enabling LANs, Wide Area Networks (WANs) or internet service providers (ISPs) to communicate with each other. Routers are continuously updating their routing tables based on the information they learn from other routers using the routing protocols.

Nowadays, fast hardware-based switches can decapsulate the packets up to application layer and can consider upper-layer information in switching decisions. This means that, in addition to routing, most of the advanced switches have built in Access Control Lists (ACL) which partly take over the role of the firewall. For example, it is possible to configure the ACLs in such a way that certain application-layer protocols are blocked or routed differently. The built-in functionality of modern switches allows the construction of the first perimeter protection layer with no extra hardware cost.

ACLs present quite important mechanisms, because failing to describe proper ACL rules might lead internet packets to go somewhere else, or, more realistically, unintended packets may be routed to our networks. This might create holes in network perimeters. ACLs need serious considerations since they have such importance, although they are not security-oriented mechanisms per se.

4.1.2 Firewalls

Firewalls are hardware or software solutions which can block unwanted traffic in networks based on predefined rules. As firewalls are able to block traffic based on port numbers, we need to clarify first what a port number means in the context of IP communication. In simple terms, each application has its own port number (like an address) on which the application service is waiting for incoming data. Looking at the ISO-OSI layering model (see Figure 1), the port number is a field in the layer 4 protocol header. The Layer 4 protocol passes the data to the service which is waiting for it on that port number. Different application protocols have different default port numbers. For example port 80 is well known as the port for HTTP (web) and port 21 for FTP. At the same time the default port numbers are not fixed, which means it is possible to configure an application service to listen to a port number other than the default one. Sometimes using the non-default port numbers is considered as a security measure, because attackers usually send malicious packets to the default port numbers.

Firewalls can be classified based on their working principle as packet filter firewall and proxy firewall. Typical packet filters check source and destination IP addresses and ports against predefined rule sets and either block or forward the original incoming packet without modifications to the next hop. Packet filter firewalls are transparent for IP communication; applying them does not change the packet headers. For instance, in order to block FTP traffic a simple firewall rule will be configured which blocks all traffic using FTP default port 21. ACL configured in a switch or a router (explained in the previous section) is actually a packet filter. In modern networks the packet filter is just a function of the perimeter router and usually separate packet filter firewalls are not used.

One typical cyber defence measure in enterprise networks is blocking all incoming connection attempts as the connections are usually established from inside to outside. This means that all incoming packets should be in response to some outgoing connection. A simple packet filter is not able to track if the incoming packet is a reply to an outgoing connection. A ‘stateful packet filter’ keeps track of connections and is able to map incoming packets to the outgoing connections and block the incoming connection setup attempts.

Unlike the packet filters, application firewalls, also called proxy firewalls, act as ‘man in the middle’ (MITM) devices. They terminate the original connection, decapsulating the

packet up to the application layer, interpreting the application protocol and formulating a new request on behalf of the initial sender. Compared to a packet filter firewall, a proxy firewall can block attacks which are built into application layer protocols like HTTP, FTP, telnet and others. The limitations for usage of the proxy firewall are complexity, supported application protocols and performance.

In addition to the above-described network firewalls which protect the whole network, there are also host-based firewalls in use. A host-based firewall is just an additional application which is installed into the host system and monitors the network connections of that host system. Most of the modern operating systems have a built-in host based firewall which can be easily turned on.

4.2 Detection and Prevention Systems

The rapid proliferation of both internal and external threats against information systems forces us to think more about traditional security measures such as ACL and firewall rules. Although those tools and techniques are major elements in our current cyber security infrastructure, there are some advanced approaches as well. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) arise at that point, and are designed to prevent advanced intrusion attempts which aim to penetrate systems.

4.2.1 Intrusion Detection and Prevention Systems

An IDS is a device or a software application which monitors network activities and operating system processes to detect potential intrusions. The IDS processes different events and logs which can be collected from one or more systems, correlating different incidents gathered from numerous servers, clients or network devices. It can be understood as an advanced monitoring technique which can collect lots of data from different nodes.

An IPS, on the other hand, has one more goal to achieve. It can also prevent malicious activities detected by IDSs. After the identification phase of an intrusion conducted by the IDS, IPSs attempt to block and stop those activities. [3] These approaches are quite similar and related, but with an essential difference. IDSs are focused on detecting incidents successfully with the lowest possible false positive and false negative rates, and reporting those activities to systems administrators in the most accurate way. It is up to system administrators to take action related to alerts, taking a second look and analysing them further, or just ignoring them if they choose. However, IPSs can be considered to be extensions to IDSs and they are more reactive. Depending on the incident, they can take actions such as sending an alarm, dropping the malicious packets, resetting the connection or blocking traffic from the offending IP address. [4]

Regarding the nature of IDS and IPS mechanisms, most of the system administrators try to balance their needs – regarding which technique they prefer – by taking into

account the complexity of the systems they manage, the number of events occurring daily, the performance of IDS/IPS tools they use and so on. For very critical production systems, IDS reports would usually suffice for system administrators, as they would not risk any automatic response which might have adverse effects.

In the following section, the modus operandi of IDS and IPS will be elaborated on focusing on different types and approaches those systems can show.

4.2.2 Signature Based *versus* Anomaly Based Intrusion Detection Systems

In order to identify an incident, IDSs use either signature based or anomaly based identification techniques. In the signature based IDS, system administrators predefine a signature which should be considered as an incident by IDS, and then IDS will only detect such incidents with those preconfigured patterns. In the signature based model, the IDS does nothing more than its predefined pattern detection. Anomaly based IDSs are a bit more active and do not need any input from system administrators. When installed, the IDS determines what is the normal behaviour of the network or a host, such as how much bandwidth is used, which ports are open, which services are running and so on. [5] After a while, the standard statistics of that environment will be learnt by the IDS. Following such calculation period, if an event occurs and has a different pattern than the expected behaviour, the IDS will report this incident as an alert.

4.2.3 Host Based *versus* Network Based Intrusion Detection Systems

Host Based Intrusion Detection Systems (HIDS) deal with host specific issues which can be a signature of an incident. They collect host data from different sources such as operating system processes and file system updates. If any incident occurs, which can be identified using signature based or anomaly based techniques as we have mentioned above, an alert is generated. Network Based Intrusion Detection Systems (NIDS) have a quite similar approach to HIDS, but they mainly focus on network activities. They can be installed at specific points in a network, which might be either a network device or a server. Then they collect network packets transmitted through those interfaces in order to identify malicious network activities.

4.2.4 Black Lists *versus* White Lists

Black list and white list techniques constitute two different approaches to security filtering. They can be implemented in IDS solutions, but it is not a requirement. Similar mechanisms can be applied to almost every information technology (IT) systems.

Black lists contain already detected IPs, hostnames, Uniform Resource Locators (URLs), processes etc. which have a relation with malicious activity. That information accumulates over time with each received internal or external data. Computer Emergency Response Teams (CERTs) can be helpful in publishing malicious IP addresses to be

blacklisted and blocked. [6] White lists, on the other hand, take the opposite view. White lists contain only necessary and legitimate IPs, URLs, hostnames, processes etc. In this approach, only listed entities are allowed to communicate, access the system, execute a certain process, or take any other action. Any other sources than the 'white-listed' ones will be blocked.

4.2.5 Deep Packet Inspection

Deep Packet Inspection (DPI) is a network analysing technique which examines the contents of network packets during transmission and can be understood as an inspection point. Results gathered from DPI node can be used just like an IDS or IPS. But using DPI might reveal more obscure malicious intentions such as advanced viruses, spam or any other content-related malevolent codes. After the inspection process, the connection which transmits that unwanted code could be terminated, or diverted to a specific network zone. The DPI technique requires lots of resources in terms of computing power. This is one of the reasons why DPI is not common compared to other solutions like IDS/IPS or firewalls. DPI can also be considered as an interception technique. Since this interception can also be done in large-scale networks, discussions about the legality of such technologies arose. If used by governments, it is a known fact that all unencrypted data transmitting in those connections can be intercepted, analysed and even stored with these DPI advancements.

DPI consumes lots of processing power, and therefore high-speed DPI equipment is much more expensive than ordinary routing equipment. DPI is often implemented at the network perimeter where all the incoming and outgoing traffic can be analysed. In case of big enterprise networks, ISPs or State backbones, the data speed in the network checkpoint can reach hundreds of gigabits per second. Until recently, even layer 3 routing of these data speeds has been a challenging task for the networking equipment, but new hardware based ASICs and multi-core processor technologies have enabled DPI up to layer 7 of terabit data speeds.

DPI technologies can serve economic purposes like network or bandwidth management. It can be used for lawful interception, copyright enforcement and for malicious data filtering. DPI can also be implemented for some more questionable purposes like for targeted advertising, and several governments are using DPI for internet surveillance and censorship. Some governments that are believed to perform DPI at State level are: Iran [7], Russia [8], China [9] and the United States (US). [10] It is obvious that the data speeds at network boundaries of these countries are very high and also huge processing power is needed for complete DPI.

In addition to processing power, there are some other limitations for the DPI and the most important one is strong encryption. [11] It is obvious that people living in digitally repressive countries are actively looking for encryption possibilities for all of their

communications. Recently several service providers (Facebook, Google) have switched to the default Secure Socket Layer (SSL)[10] encryption. Looking back to the ISO-OSI model at Figure 1, SSL is done just above layer 4. That means all network devices (e.g., switches and routers) operating below layer 4 are not even aware if the traffic they are processing is encrypted or not. After ripping off lower layer headers, the DPI platform will detect the encrypted traffic which it is not able to analyse by pattern matching techniques. Leaving the crypto breaking and bypassing aside, theoretically there is no way for a DPI platform to perform pattern matching on encrypted traffic. The easiest way some digitally repressive governments are dealing with that DPI limitation is just to throttle down or to block encrypted traffic. Other, less effective ways to deal with encrypted traffic are to perform behavioural or statistical analyses on encrypted data. For example, it is possible to detect encrypted voice over IP (VoIP) traffic based on the human conversation patterns, as the same patterns are also reflected in the encrypted network traffic. [12]

Another approach to perform surveillance of otherwise encrypted data is to perform DPI before the data is encrypted, in other words bypassing the encryption. The prerequisite for this approach is the cooperation with service providers. In case of centralised services, like Facebook, Google, Skype or many others, one encryption endpoint is centralised at the service provider's side and the other resides on the client's side. It is technically very easy to set up a DPI interception point at centralised premises of service providers. In 2013 Edward Snowden revealed the secret program PRISM. Snowden claimed that the US National Security Agency (NSA) has direct access to the servers of nine world-wide service providers in order to obtain unencrypted data for surveillance purposes. [13]

4.3 Honeypots

The term 'honeypot' has growing popularity among experts dealing with cyber security issues in the last couple of years, regardless of the expert's level of technical expertise. A honeypot can be described as 'a general computing resource, whose sole task is to be probed, attacked, compromised, used or accessed in any other unauthorized way' [14] in order to collect information about the attack and the attacker. Thus, as the definition suggests, the main task of honeypots is to be compromised in one way or another.

From a cyber defence perspective, this technique is very beneficial and useful in a couple of different ways. Honeypots can be used to collect early warning signals from malevolent actions, to analyse attacking vectors and identify what kind of attempts are coming and who might be the perpetrator, to gather different types of malwares and

[10] SSL is a protocol used for encryption of internet communication. If a web communication is encrypted using SSL it is referred as https.

0-day attacks, or even to pave the path for responsive cyber defence activities to identify persons behind malicious actions.

All of the ideas and prospective goals mentioned above can be achieved with the help of honeypots, because the intrinsic feature of these systems is to lure attackers and set up persuasive traps for them. During a cyber attack campaign, it is presumable that the actors behind the aggression are looking for vulnerable systems. Even using a single honeypot would give the upper hand to defenders because they can identify what type of offensive behaviour is taking place, what are they looking for and who they might be. Before elaborating further on the benefits of using honeypots, the technical features of honeypots will be presented.

4.3.1 Types of Honeypots

The classification of honeypots could vary depending on the point of technical resource or the level of interaction. From this perspective, attacked resources can be classified as 'server-side' or 'client-side'. There are also 'high interaction' and 'low interaction' honeypots which take into account the level of interaction of potential attackers.

Server-side honeypots are servers – which can use Linux, Windows or any other operating system which has applications and services running – which expose open ports to lure cyber attackers to interact with them. These are traditional types of honeypots, as they show most intrinsic features of these systems such as services with default passwords, easily exploitable applications and similar misconfigurations. After a login or a login attempt to those services, attackers would think they actually found a legit system and might try to take further steps such as privilege escalation and attack persistency.

The second type of honeypots, from a technical resource perspective, is the client-side honeypot. This type of honeypots uses a different approach: they crawl and probe web sites to get infected with malware in order to identify which sites have malicious codes implemented. To set up a client-side honeypot, unpatched operating systems and old versions of web browsers with vulnerable flaws are used, because they are trying to mimic novice users who have minimum knowledge about cyber security. Client-side honeypots are especially useful for CERTs to detect malicious web servers which are trying to infect their visitors, so that they can try to minimise the threats by taking counter measures against malicious activities.

Before providing examples for already developed honeypot applications, the second classification of honeypots which have two types, high interaction and low interaction, will be explained. This approach considers the interaction level between honeypot systems and attackers. High interaction honeypots let attackers gain actual high level system rights; even operating system level access could be given to attackers to watch their behaviour if they think they have compromised the machine. This mechanism needs a lot resource in terms of both physical requirements and efforts by security administrators.

For the physical requirements, such as setting up new servers with different operating systems, recent technologies help honeypot owners. Virtual technologies like products of the VMware-company, Oracle's 'Virtual Box' or Microsoft's 'Hyper-V' make things convenient, as they provide virtual operating systems so that high interaction honeypots can be installed with ease. Maintenance issues, such as creating new servers, copying them to different locations or reverting back to the initial states, take much less time. This is also important as these systems will eventually get compromised, and we do not want attackers to use honeypot systems forever.

Low interaction honeypots, on the other hand, need much less resource in terms of initial setup and maintenance costs. This type of honeypot uses fake applications which attackers might be interested in and would like to interact with. These bogus services will continue to respond to malicious requests in order to deceive aggressors to take more actions, aiming to collect as much information as possible.

The difference between low interaction and high interaction honeypots is the level of interaction they provide to potential attackers. Low interaction honeypots are easier to recognise, since they solely deal with the initial state of a cyber attack campaign, such as scanning a machine to find vulnerabilities. A low interaction honeypot can show bogus vulnerabilities, and if someone tries to exploit that specific vulnerability, this is a clear indication of a malevolent behaviour. The honeypot owner may choose to block that IP address or even report the incident to a CERT. On the other hand, High interaction honeypots do not choose to interfere that early; they instead let attackers use the machine for longer.

Although there are accepted classifications of honeypots, as mentioned above, it is also viable to think about them as a concept, and not as a collection of different technologies. As an example, we can create a fake social media account which shows an affiliation with our organization. Using that social media channel, it is possible to post fake information about non-existent systems. After some time it is possible to detect if someone uses that information, which can also be described as a honeytoken. Posting fake credit card information to hacker databases or giving out bogus account usernames and passwords to websites like 'pastebin.com' are just a few examples of this approach.

4.3.2 Honeypot Solutions

There are different information sharing portals and online forums where security experts exchange their ideas regarding honeypots. The Honeypot Project[11] is one of the most prominent examples. Academic papers as well as the newest honeypot tools and workshop announcements are shared through these portals. Project Honeypot[12] is

11 See https://www.honeynet.org/.

12 See https://www.projectHoneypot.org/.

another pertinent example in the field. Details about most of the tools mentioned below can be found on these portals.

After the theoretical discussion, it would be beneficial to give at least a brief introduction to the honeypot solutions. Despite the fact that some of them exist only for research purposes and do not last for long (because of the lack of continuous support) they are very useful.

For server-side high interaction honeypots, Argos[13] is a good example to take an initial look at. The concept behind this tool is 'to detect remote attempts to compromise the emulated guest operating system', as the authors state on their website. Another tool worth a mention is HiHAT[14]. This is a Hypertext Preprocessor (PHP) based web application honeypot that tries to detect web-based attacks such as Structured Query Language (SQL) injection, file inclusion, cross-site scripting (XSS) and so on.

On the other hand, Dionaea[15] is one of the fastest growing tools in the low interaction server-side honeypots category. The main purpose of the tool is to collect malware used by attackers, if they try to exploit fake vulnerabilities in open ports served by the tool. Even though Dionaea can handle many services in a typical box, there are also some specific tools tailored for specific ports and applications. Kippo[16] is one of them. This low interaction server-side honeypot collects information targeted against a bogus secure shell (SSH) port 22 and logs the actions taken by the aggressor after they thought they had opened a session.

Client-side honeypots constitute the second major category in this classification. Capture-HPC NG[17] is one of them. It basically interacts with servers and constantly monitors the operating system which the tool is working on, in order to detect if the connected web server tries to do something malicious. Shelia, which is another high interaction client-side honeypot, operates in a slightly different way. It clicks all links in a web page and does everything which is advertised by the web application like an unconscious user, to detect whether a malicious activity is being triggered by the server or not. Thug[18], which is a low interaction client-side honeypot, is the last example in this category. This honeypot focuses primarily on revealing malicious web pages.

Both client-side and server-side honeypots have the same aim – the detection of malicious activity – but achieve it through different means.

13 See http://www.few.vu.nl/argos/?page=1.

14 See http://hihat.sourceforge.net/.

15 See http://dionaea.carnivore.it/.

16 See http://code.google.com/p/kippo/.

17 See http://pl.honeynet.org/HoneySpiderNetworkCapture.

18 See https://github.com/buffer/thug.

4.3.3 Honeypots as a Cyber Defence Technique

After the brief introduction into honeypot technologies and available solutions, it is now possible to elaborate on these systems and discuss how they could be used to strengthen the defensive posture of an organization.

One of the main benefits of using a honeypot system is altering the phases of a cyber attack in order to extend the detection phase. There are different classifications to analyse a cyber attack life cycle. According to one them, the cycle consists of following phases: reconnaissance, weaponisation, delivery, exploitation, installation, command & control and action. It is extremely hard to detect some cyber operations during the first two phases, as the interaction between the attacker and the victim is quite low.

Honeypots can be useful in alleviating this issue. We can use honeypots to plant fake attack points to deceive attackers and this approach can be used as an early warning system. The more time the defenders have before the actual attack, the more it is possible for them to take proper measures. From this point of view, honeypots can work as an IDS/IPS system (see section 4.2.1). The difference between such solutions and honeypots is that IDSs are designed to detect actual attacks coming to real systems. Most likely they are critical production systems in an organization which means we cannot change the configuration of those systems easily, as there might be serious consequences.

Despite this obstacle, we are heavily dependent on such traditional detection mechanisms, so honeypots may provide useful solutions. Security experts can set up honeypots with the same configuration as the production servers have, but with a couple of differences. For example, honeypots will not contain critical business information, so it will not cost anything if those systems are compromised. They might have additional vulnerabilities to let attackers step into the system, in order to analyse what they are trying to achieve. If it is understood that aggressors are searching for a specific piece of information, the actual data can be moved from the real production server to another, more secure one. This type of intelligence is hard to get in the absence of honeypot systems. As a result, the possibility of remediating the time disadvantage which defenders currently suffer would help significantly with their security posture and might turn the tables against attackers.

Another useful technique which might be achieved using honeypots is connected to the challenges of attributing malicious cyber activities to an IT-system or computer network. The anonymity of the cyber attacker is a serious challenge, especially with regard to high level attacks. Finding out the real IP address or any other useful information associated with the attacker's identity is a burdensome task, although it has special importance regarding legal issues.

The honeytoken technique is another approach to get additional information about attackers and their identity, which is similar to honeypot systems. The main difference between a traditional honeypot system and a honeytoken is that honeytokens do not

have to be computer systems. They can be an email message, a text file, a web site or anything useful which might help to reveal the identity of aggressors. It is quite similar to using painted banknotes or banknotes with special serial numbers in order to track them. If someone has them, they can be easily tied to criminal activity. As an example, there are techniques where you can plant an invisible image file to a word document and whenever that document is opened somewhere in the world, the hidden image file tries to connect home, which is a web server you manage. The connection reveals the IP address of the image, as well as the document. If such documents containing critical business information are planted and distributed to different computers in an organization, then it would be possible to detect the time and place of any theft.

The third and last way of using honeypots discussed in this section is about increasing the cost of a cyber attack. Suppose there are 50 different computers, including client and server machines, in an organisation. If an attacker finds a way to connect to that network, there are only 50 machines for him to discover. Reconnaissance efforts and vulnerability scanning operations would be quite low. There are different types of honeypots which can be implemented to create fake machines in a network. Let us assume that an organisation has a B class IP range.[19] This type of setting easily allows more than 65,000 IP addresses in one network. Although there were, say, only 50 real machines, far more IP addresses could be automated to feign the 'existence' of many more computers.[20] Here the challenge for the attackers begins. Scanning all those IP addresses and receiving fake live response packets would confuse the attacker, and he would spend much more time discovering which machines are real and which are not. It is even better if high interaction honeypots are in place, because it is very hard and sometimes impossible for aggressors to recognise them as fake computer systems. Nowadays there are lots of directed attacks, but most have no specific targets. It would be fair to say that attackers, especially financially motivated ones, are looking for low-hanging fruit, which is easy to compromise without any extensive effort. Although this cannot always be the case, especially for the highly-motivated hackers, it is still beneficial to set up honeypot systems.

Increasing the cost of cyber operations for malicious users, trying to reveal the real identity of attackers and gaining additional time during a cyber attack can be listed as the main benefits of honeypot systems. Installing exploitable machines in a network[21] or planting traps for web application scanners[22] constitute different approaches to accomplishing these goals. Different honeypot solutions are very likely to increase by

19 For more information see http://technet.microsoft.com/en-us/library/cc940018.aspx.

20 One of the tools make it possible is 'Labrea Tarpit', see http://labrea.sourceforge.net/labrea-info.html.

21 Although most honeypots can be useful for this, Project Nova is worth mentioning, see http://sourceforge.net/p/adhd/wiki/Nova/.

22 Setting up such honeypots would lead web 'crawlers' and 'spiders' to go in an infinite set of dynamically generated webpages, see for example 'Spidertrap', http://sourceforge.net/p/adhd/wiki/Spidertrap/.

number and complexity. As a useful defensive technique, these solutions bring a new tool to the cyber security experts' inventory, which is likely to be effective in creating extra obstacles against aggressors.

5. Network Architecture and Security

In this section, current and upcoming security mechanisms related to network architecture will be covered. There could be a variety of different topics to elaborate on here, but a couple of most prominent ones are described in detail. Starting from air gapped networks, which are networks isolated from the internet, it will be explained what can be achieved defensively by implementing such designs. The next topic will be Domain Name System (DNS), which mainly deals with domain name to IP conversions and the security impacts of it. Then we will address a popular buzz word, cloud. In the last part of this chapter, the Internet Protocol version 6 (IPv6) protocol will be examined, which is a new protocol that has the potential to change current network designs.

5.1 Air Gapped Networks

An air gap, also known as an air wall, is a networking security measure which ensures that a computer network is physically separated from insecure networks, such as the internet or insecure LANs. [15] Physical separation also encompasses electromagnetic and electronic isolation, in order to prevent any possible data leakage from those air gapped networks. The necessity of air gapped implementations arises from the fact that the internet is a connection of networks and there is always a chance to bypass all security measures if a computer is connected to the internet. This fact remains true no matter how low that possibility is.

Air gapped networks are expensive to implement as they need extreme precaution during both set-up and maintenance. But there are other factors too. As an example, all the hardware in an air gapped network should be secure enough to prevent data leakage via TEMPEST techniques;[23] also, electromagnetic isolation solutions such as Faraday Cage should be in place.

Although air gapped networks sound quite secure, because they are isolated from external influence, there is another threat which can undermine all these measures: the human factor. Since it is very likely that an air gapped network will consist of different computers, servers, network devices or even industrial control systems, those machines use traditional media storage like Universal Serial Bus (USB) flash drives, CDs/DVDs etc. Even if there is no need to create a persistent connection to those air

[23] TEMPEST technologies refer to the different methods to collect information from emitted electromagnetic waves.

gapped networks, it is quite possible to compromise those environments with a single USB stick if it has malware in it. This is exactly what happened in Iran's Natanz nuclear facility, with the infamous malware Stuxnet. [16] Stuxnet is a very well-known example to illustrate penetration of such networks, but there might be other unknown examples. If there is human intervention, it is possible to say that all security mechanisms can be defeated. Nevertheless, air gapped networks are still strong and secure implementations compared to networks which are connected to the public internet. Numerous air gapped network examples can be found amongst military and government computer networks, financial computer systems, stock exchanges and engine control units in machines.

5.2 Domain Name System Security

The Domain Name System (DNS) is a foundational internet technology used in every name to IP conversion. Since words are much easier to remember than IP addresses like 195.222.11.253, we simply prefer using a name (www.ccdcoe.org) instead of the respective IP address. DNS provides a way to know the IP addresses of servers on the internet. It is like a directory service which provides host name–IP mappings so that we can query our desired destination. [17]

Essentially, when we want to create a connection to a server using its name, our computer tries to find which IP address belongs to that name. There are different ways to find it out. If there has been a connection to that server earlier, it is likely that our computer stores that mapping locally. If not, then the DNS starts to operate and tries to find the server's IP address by iterative or recursive queries to name servers. This process will continue until an authoritative server responds to that query and reports the IP address of the host name.

DNS attacks are trying to manipulate the host name–IP mapping process, forwarding users to wrong IP addresses. There can be different attacks against DNS, including DNS spoofing, DNS cache poisoning and DNS ID hacking, since the protocol itself does not have any inherent security measures by design. DNS ID hacking is a way to enable the other DNS attacks mentioned above. Any client waiting for a DNS reply to its query, tracks that query with an ID and if that ID is known by malicious users, they can use it and send responses with other IP addresses than the correct one. If successful, the next step is called DNS spoofing, a term referring to the action of sending false responses to those DNS requests which are intended for real DNS servers. Lastly, DNS cache poisoning is more advanced and is built on top of the other techniques we mentioned here. It is a way to poison the DNS servers' cache so that hackers can make a DNS answer to a specific request in the way they want to. If successfully conducted, these types of attacks are quite serious, since it is very difficult for even advanced users to recognise that an attack has taken place.

Although the DNS architecture seems prone to various attack vectors, as mentioned above, there are some technical security measures against those attacks. DNS Security Extensions (DNSSEC) is one of them. Basically, the purpose of DNSSEC implementation is to increase the security of name-to-IP lookup conversions by adding authentication to this process. All the queries and responses are digitally signed and this impedes DNS cache poisoning and similar attacks. DNSSEC implementation is not simple and its implementation occurs on a voluntary basis. This affects the implementation time negatively, but some countries require its use. In the US, the federal government has mandated DNSSEC implementation for government networks. Despite some promising examples, there is still a lot of work to complete DNSSEC migration from legacy systems.

5.3 Cloud Computing Security

Cloud computing security, or cloud security in short, is related to security aspects of this rapidly growing concept. Just as cloud computing itself is not only about technological advancements, but is rather a term about the concept of working with data that is accessible from anywhere and from any device, so is cloud computing security. Cloud security is related to a broad set of policies, controls, regulations and of course technological possibilities in order to mitigate different attacks coming towards the information stored in cloud computing environments.

There are different types of cloud service models such as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), and also different deployment models like private, public or hybrid. All these implementations require a different set of considerations.

From a technical point of view, cloud computing security mainly deals with virtualisation security, because the platforms under cloud services are mainly using that technology [18], but there are other issues to be taken into account. From the Information Security Management Systems' perspective, all the asset, threat and vulnerability risk assessments associated with cloud environment should be calculated carefully.

First of all, physical security of cloud devices, including servers and clients or whatsoever we want to shift to the cloud, should be under scrutiny, because the physical security of a cloud service providers' territory equals the security of the data which is stored in it. Availability, as a dimension of the CIA principles, can be also affected. Availability is important to the discussion regarding the accessibility of cloud services over the internet, since it is heavily based on the quality of the internet connections of clients and service providers.

From the confidentiality perspective, cloud services also provoke discussion because the modus operandi of this concept is about the physical relocation of our servers, and the services and applications running on them. Transmission of data from cloud service

provider to client device happens over the internet, and encryption of that connection is more important than before. Encryption mechanisms, as well as authentication techniques, require attention in cloud computing security.

Last but not least, the integrity of the data stored in cloud environments is another point to be taken into consideration. The integrity aspect also encompasses all monitoring data and logs (related to accountability), among the data itself. Since cloud service providers have access to every system in their environment with system-level access rights, they would also have the ability to access the servers they manage, and read or update data. From this perspective, cloud computing security evolves into a political and regulatory discussion. [19]

In conclusion, cloud computing security can be summarised as the sum of societies' current concerns related to the traditional security of information systems, plus the reliability and security of internet connections which are a highly dominant factor in cloud services, and the trust issues regarding the physical relocation of devices to some service providers' boundaries. Regulatory and legal issues are heavily involved in all these debates, especially the key issue of whether or not to trust cloud services and how to make them secure.

5.4 IPv6 – Solutions and Challenges

One of the most important changes which would affect network architecture and the way our devices communicate in the next few years could be IPv6. It will change the format of IP addresses which we currently use to define and identify connected machines; it will bring solutions as well as brand new questions with regard to network infrastructure. IPv6 has numerous security advancements, but they are not likely to solve every issue regarding the attribution problem or to build more resistant cyber infrastructures against cyber attacks. The following subsections deal with such IPv6 discussions.

5.4.1 Background

The proliferation of worldwide internet users and the growing number of internet-enabled devices, including smart phones, tablet PCs, watches, cars or even household devices like fridges, ovens and air conditioners, require a unique identifier for each to connect and communicate with each other, which is called an IP address.[24] Obviously it is not enough to have just an IP address to connect this massive network of networks; there should also be a protocol which handles the assignment of those IP addresses and describes how they operate with each other. IPv6 deals with this issue to make the internet work, just like its predecessor protocol, Internet Protocol version 4 (IPv4).

24 See *supra* note 4.

Since every device which joins the internet needs a different IP address, protocols should have sufficient unassigned IP resources to fulfil these demands. The need for IPv6 arose from this point, since IPv4 uses a 32-bit address space which can distribute up to 4,294,967,296 unique addresses [20], which has already run out.[25] Reports indicate that there are 2.7 billion people online [21], and the number of internet-enabled devices is today more than 10 billion [22]. IPv6 uses 128-bit address space which can be used to distribute 34x1037 IP addresses (number 34 followed by 37 zeros). This huge number is more than enough for now and for the foreseeable future.

5.4.2 Technical Insights

Before we take a closer look at transitional issues and the management of IPv6, we will discuss the technical differences of IPv6 and related security issues first. One of the key elements of IPv6 is related to its new network topology. This is the arrangement of various elements including switches, hubs, routers and client computers. Since IPv6 makes it possible to use many more IP addresses thanks to the vast IP address pool, the need to create subgroups (LANs, Virtual LANs etc.) will decrease. The restrictions related to the assignment of IPv4 addresses would not be an issue anymore. This situation would also affect the topological design of other network devices, such as routers and switches. Connections between two end-user computers would be mediated by fewer such devices. As a result, attackers would find more chances to initiate direct connections with their victims.

One of the major issues regarding IPv6 is about Router Discovery (RD) operations. In order for a router to establish a connection to the rest of the world, an IPv6 enabled device first needs to discover that router. This is done via a special message which requests that information for the router. If an intruder manages to install itself in the same network as that device, there is the possibility to send a fake response message. If successful, the connection between the device and the router might be intercepted and this results a Man-in-the-Middle (MITM) attack.

Another feature worth mentioning about IPv6 is its native support for Internet Protocol Security (IPsec). IPsec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a communication session.[26] IPsec provides various security services to achieve data confidentiality, data integrity and authentication at the network layer. Details about layering model and encapsulation can be found in section 3, and insights about how encryption works will be elaborated on in section 6 of this chapter. As a short summary, IPsec provides authenticity for every

25 Although IPv4 protocol has already run out of available IP resources, we can still use IPv4 due to solutions like Network Address Translation (NAT) protocol. Using the NAT protocol allows to share a unique IP address with different users in an internal network to access the internet. 192.168.X.X type of IP addresses constitute an example of those private addresses.

26 See Internet Protocol Security, http://en.wikipedia.org/wiki/IPsec.

piece of data which is transmitted over the network (IP packet), by check-summing the packages using a cryptographic hash[27] algorithm. IPsec works well both for IPv4 and IPv6, but there is a difference. IPv6 provides native support for IPsec because IPsec was originally developed for IPv6, but found widespread deployment in IPv4 first.

The vast address space brings different concerns as well. One of them is reputation-based protection services. These services or lists are being used to prevent known malicious servers from passing defensive perimeters by blocking them beforehand. There are both public and private services which offer these solutions. This technique works with black lists and calculates whether a server has a good reputation to access a specific resource. IPv4 reputation lists have a wide collection of IP addresses in them, because of the time spent with IPv4 protocol. IPv6 has not yet comprehensively identified malicious IP addresses. Even though we might think it is because the usage rates of IPv6 are not yet mature, there is another reason why these services may be compromised: the vast address space of IPv6. Since there are trillions upon trillions of IP addresses available in IPv6, collection and distribution of malicious IP addresses is a daunting task. Malevolent users can easily change their IP address to continue their work without interruption and avoid getting caught on a reputation list. From a defensive perspective, it can also be tricky to manage servers with more than one network interface and simultaneously deal with different network schemes. Different network interfaces can offer different IP addresses to a server in order to establish internet connection and this situation prevents security administrators from correlating malicious activity between a server and an IP address. Attackers can use one server with tens or even hundreds of IP addresses, without having to worry about moving their 'artillery' to another server.

IPv6 IP addresses would also bring difficulties to security monitoring systems and their operators. One reason is the syntax of the new type of IP address. Logging systems can fail to detect them, as one IPv6 addresses can be written in numerous ways. Also, traditional logging mechanisms and even IDS/IPS systems use grep-like[28] commands to match certain events. As an example, an IPv6 address can be written in the following ways:

2a4f:0000:0000:0000:0005:0600:300c:326b

2a4f:0:0:0:5:600:300c:326b

2a4f::5:600:300c:326b

27 A cryptographic hash function is a process that computes a value (referred to as a hashword) from a particular data unit in a manner that, when a hashword is protected, manipulation of the data is detectable, see http://www.techdictionary.com.

28 This 'grep' command is used to match a certain pattern of characters from an input, such as a text file. Logging mechanisms are heavily dependent on this kind of basic but powerful detection mechanism. For more information see http://www.unix.com/man-page/OpenSolaris/1/grep.

The IP addresses listed above are actually same, but they are formatted differently. The main reason for this is the convenience of reading and writing shorter words, or IP addresses in this case. There are no shortenings like this in IPv4, which makes it a lot easier to filter and match IP addresses. As an example, 192.168.1.2 is always written as it is. There is no necessity for shortening IPv4 addresses as they are already short and easily writable.

Another burden for the monitoring solutions is the difficulty of technical implementation. Security Information and Event Management applications are heavily based on IPv4. Considering that the numerous already developed open source tools and commercial off-the-shelf (COTS) software products are based on IPv4, both the technical research and implementation for IPv6-type monitoring solutions will be time-consuming and difficult to achieve in the near future.

5.4.3 Transition to IPv6

Transition to IPv6 and the possibility of achieving pure IPv6 for the internet is a subject long argued over. Although there are concerns about address exhaustion of IPv4, migration deadlines for IPv6 have been repeatedly postponed to undetermined dates. There are reasons behind this which were explained in section 5.4.2, such as using Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) technologies to share one public IP in order to access internet from an inner domain.[29] Starting from 2011, IPv6 adoption rate has grown steadily worldwide. Statistics show that IPv6 support is almost 2% as of today. [23].

The transition to IPv6 brings different questions, such as whether the transition will ever be concluded and whether IPv4 will disappear. Experts have different opinions, but most of them believe transition itself can be a pitfall. Since IPv4 and IPv6 are not compatible and it is not possible to use them together without Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), Teredo or 6to4 packet converting techniques, IPv4 and IPv6 will inevitably result in middle boxes mediating transactions through networks. This situation would create a double attack surface, and it would be harder to defend both. Another issue is that, although IPv4 and IPv6 have different strengths and weaknesses in terms of security, attackers would have a chance to penetrate whichever is more susceptible to attack. From an attacker's perspective, it is likely that options will double in number. Unfortunately, from the defender's angle, the number of things to protect would increase as well.

Another problem related to the transition is that IPv6 may operate by default in different environments and configurations, which may generate some drawbacks. It would be very likely that end users or even administrators dealing with systems and network

29 Technologies like DHCP and NAT make it easier to share a single IP address across a network, an organization for example. Thus, multiple clients can use the same IP address for internet access.

operations might not be aware of IPv6-related security hardenings. As a result, we could see many systems with improper configurations. This would help attackers to find security holes, especially in the complex environments, which might lead to misuse of those settings. It would be possible for them to use IPv6 properties and bypass IPv4 security features or hardenings.

Both the native IPv6 support and other workaround solutions like Teredo, ISATAP and 6to4 require additional effort and most network administrators would perceive this phase as an extra burden for their daily work. IPv4 has lots of security solutions which are either developed in-house or offered by providers, and are tailored for each specific system. On the other hand, there are only few IPv6 tools, technical guidelines and solutions available. This would inevitably lead to additional learning and development efforts for system administrators, so malicious users can benefit from this phase to exploit poorly known vulnerabilities. The nature of migrating to a new and different technology would bring new opportunities, but attackers are the first to use them.

5.4.4 Management Issues

IPv6 comes with a couple of managerial issues as well. Most of them are related to the decision of how and when to commence the transition period, and when to end it. Although it would be required for future implementations of the internet, some executives think that there are no compelling reasons to conclude the transition phase early. The reason of that is, if operations in a company are working flawlessly, a major upgrade in the environment could bring lots of risk. There will be some services which require IPv6 in the near future, but if they are not crucial for companies, then there is no motivating reason to finish the transition as early as possible.

Another issue regarding transition management could be the cost of devices, technological investments and training of employees. There are few people in the market who know the technical details and also possess adequate experience in IPv6. From a managerial perspective, shifting to IPv6 would require acceptable numbers of high-quality personnel to lead the transition, especially for big companies and organisations. Otherwise, it is likely that mistakes will occur during and after transition. Both training the already available personnel and hiring IPv6 experts would be costly. This is one of the reasons why some companies do not list IPv6 readiness as an important item in their future plans.

Another point worth considering is the IPv6's extensive address space. Although it might make it difficult for attackers to scan a network to find vulnerable machines, it is also hard to manage those networks. Maintaining proper configurations of machines in such a complex infrastructure in terms of IP space would be a daunting task for network administrators. There should be intense controls and active measurement systems in order to keep the environment up to date and under control. Even in current

IPv4 environments, managing network topologies is not an easy task, especially taking into account different segmentations such as production servers, 'demilitarised zone' (DMZ) servers, and dedicated segments for applications facing the internet. Using 128-bit addressing in IPv6 together with IPv4 addresses would require lots of resources to manage systems appropriately. As an example, in real deployments, it is common for each endpoint in a network to have a 64-bit address space. There may be only a couple of active nodes, but even that address space is over 4 billion times the size of the entire IPv4 internet. This would force network administrators to create shortcuts, both for assigning IPv6 addresses to end nodes and subnets in their IP range. This might help attackers because if the addressing mechanism is understood by them, reconnaissance efforts would reduce dramatically.

It would be fair to say that IPv6 would bring some new features which can be useful for the security posture of an organisation, but it has also some drawbacks. Especially during the transition phase from IPv4 to IPv6, we might face additional techniques which attackers tend to use in those systems. While IPv6 comes with additional security-related features, such as IPsec and IPv6 vast IP space, there will also be lots of new ways of and possibilities for finding weaknesses in networks. IPv6 might help catch basic attacks coming from novice hackers, but it is very likely that advanced attacks would continue to exist, especially because clever attackers will always find a way to get into the networks no matter whether it is using IPv4 or IPv6.

6. Encryption

This section does not cover the mathematics which lies behind all cryptographic algorithms; however, in order to analyse the limits related to encryption, the topics of symmetric encryption, asymmetric encryption, and hashing each will be covered in detail. Two different encryption purposes are covered: encryption of data in transit and encryption of data at rest.[30]

6.1 Symmetric Encryption

Symmetric encryption algorithms use the same key for encryption and decryption. One of the strongest publicly available symmetric encryption algorithms nowadays is the Advanced Encryption Standard (AES)[31], which is available in 128, 192 or 256 bit key length. That means the same binary key of 128, 192 or 256 bits is used for encryption and also for decryption. The users are capable of remembering passwords and passphrases used as an encryption key, but not the 256-bit long binary bit streams

30 The term 'data at rest' is used for the data stored in local environment and not sent to anyone. The term 'data in transit' refers to data sent over the network to a communication partner.

31 AES is a symmetric encryption algorithm established by the US National Institute of Standards and Technology (NIST) in 2001.

consisting of 256 zeros or ones. It would be possible to convert the 256-bit binary key to 16 hexadecimal numbers, but even that is, for most humans, difficult to remember. Hashing can be used to derive the fixed length binary key from any easily memorable password or passphrase.

Hashing is a one-way mathematical function of converting a text of any length into a fixed length value consisting of ones and zeros (hash value). Some of the important properties of hashing are:

- it produces always the same hash value from the same plaintext;
- it is a one-way algorithm: it is not possible to derive the original text from the hash value;
- changing the original text even by a single bit gives a completely different hash value;
- it is extremely unlikely[32] that two different plaintext messages will give the same hash value (collision); [24]
- it is practically impossible[33] to compose a plaintext which would return a desired hash value after applying the hash process to the plaintext.

So hashing is the perfect function to retrieve the required binary key from the password or passphrases. The symmetric encryption-decryption process with passwords would look like the following:

Encryption:

1. Using a hash algorithm, the password or passphrase is hashed, giving a fixed length hash value.
2. Hash value is used as an encryption key for the encryption of the plaintext in order to get the encrypted cipher text.

Decryption:

1. Using a hash algorithm, the password or passphrase is hashed, giving a fixed length hash value.
2. Hash value is used as a decryption key for the decryption of the cipher text in order to get the plaintext.

If symmetric encryption is used to encrypt data at rest, then key management is not an issue. We just need to remember the password which was used at encryption and use the same password for decryption.

32 'Extremely unlikely' in this context means that although the collision is theoretically possible, its probability is so low that in any practical implementation it shouldn't be considered.

33 Term 'practically impossible' in this context can also be understood as 'extremely difficult'. Although theoretically it would be possible, using nowadays available computing power it cannot be expected that someone is able to accomplish the task in a reasonable timeframe.

If symmetric encryption is used for data in transit, there is a need for a secure key transmission to the other communication partner who needs the same key for the decryption of the message. Sending the symmetric key to the communication partner might be challenging as encryption keys may be eavesdropped or manipulated during transit. Luckily, nowadays there are several tamper-proof key exchange methods available (e.g., Diffie–Hellman, RSA[34]), and sending the key is not the main problem with symmetric encryption.

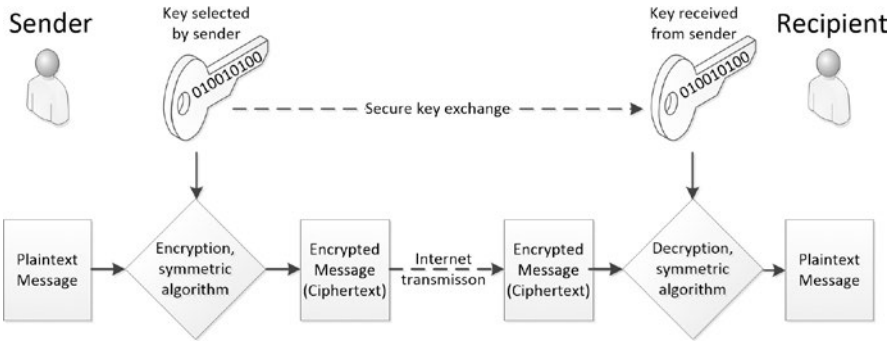

Figure 4. Symmetric encryption-decryption process.

If we use symmetric encryption for data in transit, theoretically we should have different keys for each communication partner. If everyone must have the ability to send an encrypted message to everyone else (e.g., for corporate email encryption solution), a huge number of different encryption keys need to be exchanged and managed. Therefore the key management of symmetric keys would become an unrealistic task already with even a relatively small number of communication partners.

6.2 Asymmetric Encryption

Asymmetric encryption gives a solution to the problem of managing the huge number of keys and for the authentication of communication partners. A mathematically linked key pair is generated. A typical length of the asymmetric key could be 2048 bits, which is around ten times longer than the key size of a typical symmetric encryption algorithm. Longer key size also makes the asymmetric encryption more resistant to 'brute-force' attacks, but that is not the main reason for using it. A more important difference is that two keys are used in asymmetric encryption. One key can be used for encryption and only the other key from the same key pair can be used for decryption. Generally, the keys in the key pair are equal, just one of the keys (public key) will be made public

[34] Both referred secure key exchange methods are explained in detail in Microsoft Technet, see http://technet.microsoft.com/en-us/library/cc962035.aspx.

and can be published in directories. For example, the hash value of the public key can be printed on business cards. The other key of the same pair will be kept secret and is known only by the owner. This key is called either a private key or a secret key.

Two different use cases can be realised by asymmetric encryption algorithms. First, if the plaintext is encrypted by using the public key of the recipient (see Figure 5), then only the recipient can decrypt the message using his private key. This is the typical scenario used to provide confidentiality for the data in transit. The private key of the recipient provides the confidentiality.

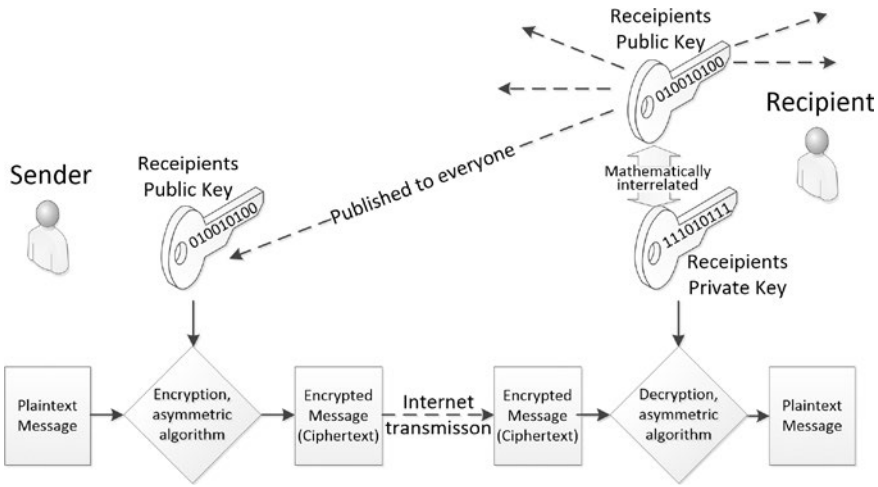

Figure 5. Asymmetric encryption-decryption process.

The second usage scenario of asymmetric encryption is the digital signature (see Figure 6). The hash value of the document is encrypted using the private key of the sender who is signing the document. In this scenario the document itself can be sent to recipient without any encryption. The recipient decrypts the sender's hash using his public key and compares the sender's hash value with the self-calculated hash value. If the two hash values match, then it proves that the sender, as the owner of the private key, has signed the document and the text has not been altered during transit.

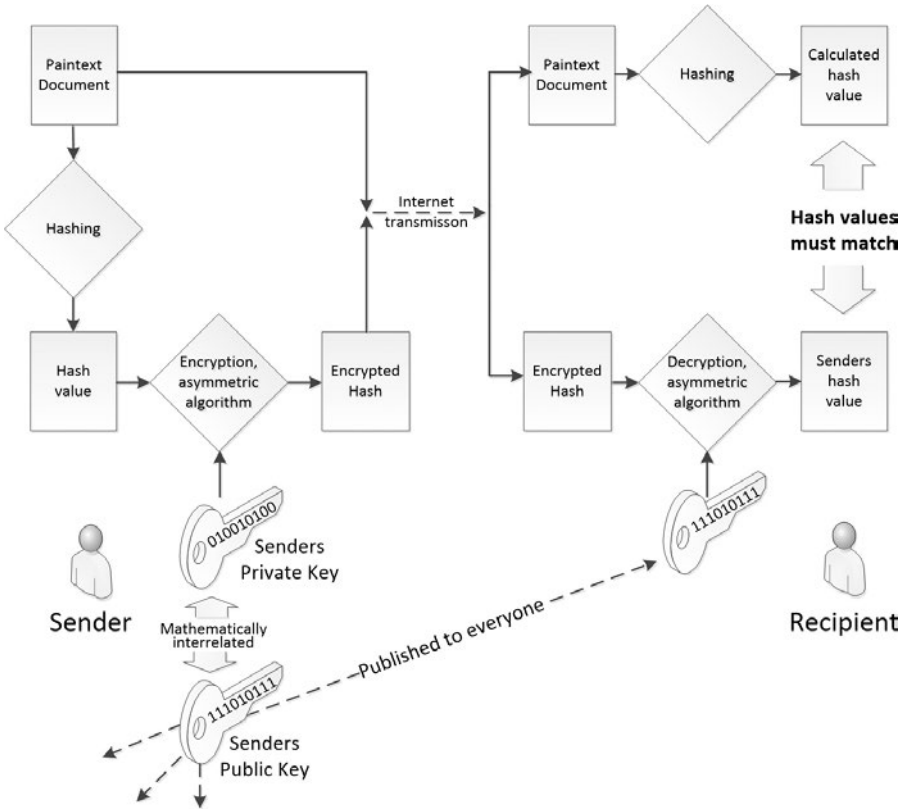

Figure 6. Digital signature process.

In the case of asymmetric encryption, the same key pair assigned to a user is used for all parties communicating with this user. Therefore, the compromise of the private key would be fatal for a given user, because the compromise would affect all of his or her communication partners. In symmetric encryption, the compromise of one key would affect only one communication relation of the user as a different key is used for other communication parties.

One implementation detail to consider is that asymmetric encryption process consumes around 1000 times more processing power than symmetric encryption. In other words, asymmetric encryption is slower than symmetric encryption. This might present practical challenges to the encryption of fast data streams in real time by asymmetric algorithms. Luckily, there is a workaround for that problem where only a short session key will be encrypted by asymmetric algorithm and then the messages are encrypted by symmetric encryption algorithm using the session key. This is called a hybrid

cryptosystem and nowadays most of the asymmetric encryption implementations are hybrid cryptosystems.

	Symmetric encryption	**Asymmetric encryption**
Number of keys	Same key for encryption and decryption	Two mathematically linked keys forming a key pair. One key is used for encryption, the other key is used for decryption
Speed	Faster, requires less computing power	Slower, requires more computing power
Typical key length	56–256 bits	1024–4096 bits
Key exchange	Does not scale	Scaling is not a problem
Sensitivity for compromise	Only one communication relation affected if key is compromised	Affects all communication relations of the user if private key is compromised
Suitable scenario	Data at rest	Data in transit
Sample algorithms	AES (128, 192, 256-bit key) Blowfish (32-448 bit key) 3DES (112, 168 bit key) DES (56 bit key)	RSA (1024–4096 bit key) ElGamal

Table 1. Comparison of symmetric and asymmetric encryption.

6.3 Limits of Encryption

After having covered the basics of symmetric and asymmetric encryption and hashing, this section will cover some practical problems and limits related to encryption.

First, it is important to understand that the user-defined key or password provides the secrecy of the message, not that of the encryption algorithm. The encryption algorithm itself and the source code of the implementation software can be public or proprietary, and public algorithms have some benefits over proprietary ones. If the encryption algorithm is public, then the cryptographic community is able to analyse it for vulnerabilities. By vulnerabilities we mean findings which allow the encrypted message to be broken faster than by 'brute-force' attack. Usually, the vulnerabilities found are theoretical and might weaken the algorithm only a little. As an example, a vulnerability in an algorithm may reduce the strength of an encryption algorithm with a 256-bit key length by a few bits, making it comparable to, for instance, a 254-bit key length. This does not have much practical value because the algorithm with 254-bit key length would also be considered unbreakable. Usually the cryptologists publish new vulnerabilities, but there is a theoretical possibility that some vulnerabilities are not published and may be kept confidential by, e.g., intelligence agencies.

Theoretically, it is possible to break any encryption by 'brute-force' attack. This could be achieved by trying all possible combinations of the encryption key. The main constraints with this approach are time and the computing power which can be obtained for the money available. [25] For example, AES is currently considered to be the most secure public symmetric encryption algorithm. It is available with 128, 192 and 256-bit key length. Obviously, the 256-bit version is considered to be stronger than the others, because the longer key is more resistant to 'brute-force' attacks. A key with 256-bit length has 2^{256} possible combinations and it would take an unimaginable number of years to break it by 'brute-force' attack using contemporary computing power. The information would lose its value by the time a 'brute-force' attack had been successful. Some may argue that we should also consider Moore's law,[35] which states that available computing power doubles roughly every 18 months. This is an observation which has been more or less true for around 25 years, but the trend might not continue like this forever. Even considering Moore's law does not change the situation radically. There is not much practical difference in cracking an AES 256-bit key by 'brute-force' in 1050 years, or in a hundred years less.

Another observation is that the Data Encryption Standard (DES) symmetric encryption algorithm did stand for 25 years until it was cracked by 'brute-force'. [26] How long will the AES stand, which was published in 2001 and is considered to be the best symmetric encryption algorithm available? Today we know only that AES does not have any publicly documented cases of breaking. It is also claimed that some intelligence agencies are storing the encrypted messages hoping that the new technologies developed in future will allow the encryption to be broken before the information loses its value. [10] One of the new technologies which in future could potentially crack the encryption is quantum computing.[36]

A second and even more complex issue is related to the secure coding of cryptographic software. Again, there is open source software and proprietary software available and the same logic applies that open source cryptographic software is considered to be more secure because it would be more difficult to hide backdoors. There are several claims that intelligence agencies are putting pressure on software vendors to implement backdoors into encryption software. [27] Obviously, open source software would be more resistant to this kind of attack, but it is still possible to hide backdoors in open source software.

The third issue to consider is the encryption endpoint and the layer where the encryption is done. We need to distinguish between end-to-end encryption on the one hand, and scenarios where an encrypted channel is established between the end-user and a server,

35 Gordon E Moore described the trend of developing computing power in 1965, see http://en.wikipedia.org/wiki/Moore's_law.

36 For more information on quantum computing see http://en.wikipedia.org/wiki/Quantum_computer.

or between the end-user and the network perimeter, on the other hand. A typical example without end-to-end encryption is a corporate Virtual Private Network (VPN) where one end of the encrypted channel is terminated at the end user PC and the other at the border of the corporate network. The VPN extends the corporate network virtually to the remote client through an encrypted tunnel which is routed over the internet. As the encrypted tunnel is on top of layer 3, the client will get the IP address from the corporate network and virtually remains within the borders of corporate network. Different applications running on VPN-connected clients establish their own layer 4 connections to the outside servers via corporate gateways. In this encryption scenario, the administrators of corporate networks are able to monitor all the traffic of the VPN-connected client because the traffic is encrypted only to the border of the corporate network.

Another example explaining the encryption endpoint problem is SSL encryption where each application connection is encrypted separately at layer 4. If a web browser initiates an SSL connection to the web server, the connection between the client application (e.g., a web browser) and the web server is encrypted. The client also asks for the certificate of the web server and checks if the signed certification authority (CA) is in the list of trusted CAs of the client. In the case of SSL encryption, the network administrators would not be able to monitor the traffic; for this reason, it is called end-to-end encryption. One of the main risks related to encrypted SSL connections is the MITM attack. In this scenario, the SSL connection from the client is rerouted to a proxy acting as the 'man in the middle', and is terminated there. The proxy establishes another SSL connection to the web server. As the encryption would be broken at the proxy, the owner of the proxy could monitor the unencrypted communication. This attack has the problem that the certificate presented by the proxy would not be signed by a trusted CA and the browser would warn of the untrusted connection by a red address bar or a popup message.

There is a way that the client can verify the identity of the server he intends connect to. The server sends its certificate to the client. The server's certificate proves that the URL belongs to the certificate holder and is digitally signed by a party which is trusted by the client. If there is any mismatch between the data of the browsed web page and the certificate (for example if the URL is different), the browser displays a warning, which is a sign of a possible MITM attack. Clients (web browsers) have a built-in list of trusted CAs. Usually, browsers have several default entries for the biggest CAs in this list, but the list can be extended by the administrator of the client. A typical MITM scenario in governmental and corporate networks where the routing, proxy and the client system are controlled by the same organisation is:

1. SSL traffic to the web server is routed to the proxy by network administrators.
2. The proxy presents a fake certificate to the client which is digitally signed by the organisation itself.
3. The organisation who signed the fake certificate has been entered into the list of

trusted CAs of the client by system administrators who have full access to client configuration anyway.

4. The connection from client to proxy does not show any warning, because the digital signature of the presented certificate is trusted by the client.
5. The proxy establishes another encrypted connection on behalf of the client to the web server and mediates the plaintext between the two encrypted connections.

This very typical scenario, also called SSL inspection, enables an organisation to monitor the SSL connections without any warning being presented to the user. However, a skilled user would be able to check the details of the certificate and find out that it is signed by the organisation itself.

Several communication services (chat, email, VoIP and others) are set up in such a way that each client is communicating with the server over an encrypted connection terminated at the server, and the server commutates the messages between the end users. In this case, the service provider has full access to the plaintext communication of all users. That is why governmental intelligence agencies have an interest in cooperating with service providers in order to have direct access to the unencrypted communications between customers. In 2013, Edward Snowden revealed the existence of PRISM, a secret cooperation program of the US NSA, with nine worldwide service providers. [13]

6.4 Interim Conclusions

One of the simplest ways to send a secret message over the internet is just to compress the file and encrypt it by 256-bit AES encryption, using WinZip and a strong password. Then the zip file can be sent over the public networks by email. Many users are using this method; this was also the official recommendation of the US NSA. [28] In this scenario, it must be considered how the password is sent to a remote recipient. Quite often the sender calls the recipient and tells the password over the phone. This would leave additional risks if someone eavesdrops the phone call and thus would learn about the WinZip password. Following the typical encryption scenario described here, we would have to consider some issues we know and some others we do not: [29]

- We know that cracking a 256-bit long key of AES algorithm by ‘brute-force’ would take an unimaginable amount of years. This is not a realistic attack scenario today.
- We know that there are no published vulnerabilities in the AES algorithm which would remarkably reduce the time needed for cracking the message.
- We do not know if NSA or any other person or organisation has found an unpublished vulnerability in AES algorithm which would allow cracking the encryption. This is rather unlikely, as AES is open source project, but we cannot completely exclude this possibility.
- We do not know if there are any deliberate or non-deliberate backdoors or vulnerabilities built in into WinZip which would allow cracking the encryption.

This is more likely, because WinZip is not an open source software, which makes the auditing of the code more difficult.

To summarise, the weakest link is probably not the encryption algorithm but the implementation of the entire cryptosystem: the design of the encryption software, the coding of the algorithm, key management, password leakage and so on.

7. Organisational Aspects of Cyber Defence

7.1 Internet Organisation

This section will show how the internet is organised and how it works technically. Further, the potential power of organisations will be assessed, especially with regard to the ability to shut down the internet.

ISP are organisations providing internet services to end users. Historically, they are the telecommunication companies who, in addition to supplying telephone services, now also provide internet services. They offer either physical or radio connections to end users. ISPs also provide IP addresses and routing information to and from the end user's host or network. In order to provide the service to end users, the ISPs must also have internet uplinks to other ISPs. ISPs are sometimes divided into tiers (tier-1, tier-2 and tier-3) depending on whether they pay fees for the interconnections with other networks or they just peer[37] on a voluntary basis with other networks, and maybe sell connectivity to others. Tier-1 networks are the few largest networks which are believed to have access to every IP address based on peering relations alone (i.e. no payments are involved).

Routers in the internet permanently share their routes with neighbours and also learn new routes from them. That is done by means of routing protocols, whereby routing information is transferred in parallel to productive traffic. Recently, several discussions have taken place about whether and how it would be possible to shut down the entire internet or to disconnect one country from the internet. As the internet is a distributed system, there is no single political power that could impact the whole internet. The possible political risk to the internet of a single country depends on the number of ISPs in the country [30] and the number of physical external connections.

Technically, there are two major options for disconnecting a country from the internet:

- The first and the most straightforward possibility is simply to cut the wires at the borders. This should not affect internal connectivity within the country, but integrated services today heavily depend on external connections. For example, several social networking and peer-to-peer communication solutions would not work, as they have a client-server communication model which does not function if communication to the server located outside the country is broken.

37 Peering is a voluntary and free of charge interconnection of administratively separate internet networks.

- Another and more selective solution is blocking routing updates at the border routers. There would also be a possibility to reconfigure the DNS, but this would not cause a complete shutdown because the routing and connectivity on the IP address level would remain unaffected. In order to block the routing advertisements at the border router, all ISPs would have to act. If a country only has a few, government-controlled ISPs, the probability for this kind of shutdown for political reasons is high. This has happened in Egypt and Libya in 2011, and Syria in 2012. [31] If the number of externally connected ISPs operating in the country is very high, the risk of political internet manipulation is lower.

7.2 Domain Name System Organisation

As explained in section 5.2, DNS is the system which converts the URL names into a routable IP address. The DNS is a hierarchical system where the Internet Assigned Numbers Authority (IANA), operated by the Internet Corporation for Assigned Names and Numbers (ICANN), is responsible for management of the Top Level Domains (TLDs). There are two kinds of TLDs: global TLDs like '.com', '.org' and country-specific TLDs, such as '.fr' (France) and '.ch' (China). The central part of the DNS are the root name servers operated by 13 operators who provide root name service by 13 unique IP addresses. The root name server operators are international organisations headquartered all around the world, although eight are US organisations.[38] The limit of 13 IP addresses comes from DNS protocol and cannot be extended. However, a network addressing and routing methodology named 'IP anycast' technology allows a distributed architecture to be built behind a single IP address. Nowadays, the 13 root name server operators have built a distributed network of root name servers with, as of 13 November 2013, 386 servers[39] around the world. For a service user it means that the closest server will reply to a request.

The root name servers are updated regularly by distributing the root zone file prepared by IANA/ICANN. The file itself is distributed via hidden distribution servers. The addresses and locations of these servers are not published to avoid targeted cyber attacks. The root name servers download the root zone file and the operators must check the authenticity of the root zone file before applying the changes. That is done by digital signature. IANA/ICANN is responsible for the administration of the TLDs, but all changes in the root zone file must be approved by the US Department of Commerce, making the US government the ultimate authority for the DNS. In this kind of hierarchical DNS setup there is one ultimate authority that has the power over the TLDs. Currently that power is in hands of ICANN but the US Department of Commerce has a right to veto changes to be introduced in the TLDs.

38 See http://www.iana.org/domains/root/servers.

39 See www.root-servers.org.

There have been several debates about whether this hierarchical DNS setup could introduce any political risks for internet operations. Technically the Root Name Servers are distributed and the process of the root zone file distribution is also pretty reliable. On the management side, ICANN itself has proven procedures for implementing any changes. As in any other hierarchical system, the root has a biggest potential impact to the whole system and might be the most rewarding target for any attack.

7.3 Information Security Management System

Each organisation which pays attention to information security governance should have a management-approved Information Security Management System (ISMS) in place which defines the security objectives, processes and methods to achieve the targeted level of overall security. ISMS is a framework which helps to implement and assure the overall information security governance in the organisation.

ISMS defines the methodology of how to define the assets which are relevant for information security, how to select security controls, how to implement them and finally how to audit their effectiveness. Organisational ISMS can be based on a national (e.g., US NIST SP800-37 [32], German BSI [33] and Estonian ISKE [34]) or an international standards (e.g., ISO/IEC 27001 [1]).

Alternatively, an organisation can develop its own tailor-made information security ISMS addressing organisational requirements. However, deploying an ISMS which is based on international ISO/IEC 27001 standard gives much better transparency for all partners and especially for customers. This is because it is possible to audit and certify the organisational ISMS based on the ISO/IEC 27001, which provides certain assurance to external stakeholders about information security governance within the organisation.

Besides defining the general information security lifecycle and related processes, one of the issues an ISMS deals with is the specification of the assets which are considered relevant for information security in a given organisation. Depending on the organisation, these assets may include data, servers, clients and networks, as well as rooms and buildings. The next task is to define the risk management methodology for the organisation and to estimate risks for the identified assets. As an input for the risk estimation, we need to estimate the threats and vulnerabilities and the impact of a possible security breach. Often, it is not easy to have very precise input data for risk estimation and therefore a qualitative risk estimation methodology could be applied which gives risk levels (e.g., low, medium, high). The next step in implementing the ISMS would be the development of security controls which would mitigate the risks to an acceptable level. Depending on requirements, security controls can be selected and adapted from a catalogue, or alternatively tailor-made security controls can be developed for more specific control areas. At this point, the costs and impact analysis of the security controls is also done. The target of the analysis is to find the cheapest

controls which will give the biggest positive impact. Typical examples of the security controls are data encryption, access control, segregation of duties in working processes, requirements for server rooms, and hundreds of others. After these analytical steps, the implementation of the security controls starts. Often, many security controls already exist, and only the missing part needs to be implemented. The implementation of security controls is followed by periodic auditing and continuous improvement, making the managed information security a continuous process.

This managed information security process provides a conscious and cost-optimised way to improve information security in an organisation. At the same time, it does not give any guarantees of avoiding serious security incidents. Bad things can happen even in the organisations best at investing money and taking care of information security, just the incident probability will be lower than in other organisations with a more ad hoc approach to information security.

7.4 Secure Software Development Life Cycle

One of the major problems in today's cyber world is application vulnerabilities.[40] Discovering those vulnerabilities and writing malicious codes to exploit them would lead to unauthorised access for hackers. In order to prevent this, software developers perform security assessments of applications after they have developed their products, but it is very likely that they will not find every flaw in a specific application. After product release, hundreds or even thousands of researchers will continue to test that application to see whether it has a security flaw. If a hacker finds a vulnerability and manages to implement an exploit code for that flaw, then the situation constitutes a quite serious problem. After this stage, there is one thing left for developers to prevent someone using that flaw; patching the software and releasing a new version. Unfortunately, it may not work out as expected. Upgrading software with a new version is both time consuming and hard to manage, especially in corporate environments. In order to prevent such 'find the flaw – patch the flaw' loop, Secure Software Development Life Cycle (S-SDLC) could be used to develop products with significantly less vulnerabilities.

Before elaborating on S-SDLC, giving a brief definition about Software Development Life Cycle (SDLC) would be beneficial. SDLC is defined as the process which is followed to develop a software product.[41] It includes several major steps; requirement identification, design, coding, testing and deployment. Every step has a crucial role and the potential to affect the quality of the final product. On the other hand, there are other issues to be solved in order to produce 'secure by design' software products. The S-SDLC approach aims to provide solutions to this problem. S-SDLC proposes

40 An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application, see http://www.veracode.com/security/application-vulnerability.

41 See http://resources.infosecinstitute.com/intro-secure-software-development-life-cycle/.

security-minded development steps and suggests software development companies to consider security aspects of a product in each phase of development. An example for an S-SDLC process is shown in Figure 7. If every phase is successfully completed, taking into account the product specific requirements, then the chances of discovering vulnerabilities after the product release will decrease dramatically.

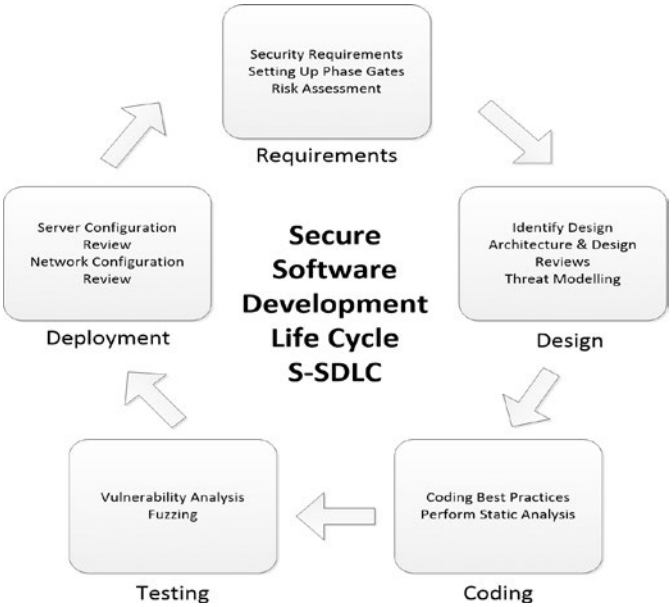

Figure 7. Secure Software Development Life Cycle.

Although this S-SDLC process would help to develop far better products in security terms, implementation of this cycle is quite difficult for every application. The main reason behind this unfortunate fact is budget constraint. Every additional step requires much more effort, which will affect the overall cost of the project as well as the time required to complete it. There might be other unavoidable limitations to implement S-SDLC in some cases, but it is very likely that most of the software development processes simply ignore using such detailed and expensive procedures.

8. Summary

In this chapter some of the most critical cyber defence issues have been analysed by virtue of technical aspects. Traditional defensive mechanisms such as firewalls and Intrusion Detection & Prevention Systems, as well as general information about

security objectives were described. Supporting these technologies, the nature of internet and data transmissions over network connections were also introduced briefly. After describing these technical solutions, upcoming technologies, with the challenges and solutions they bring, were elaborated in detail. IPv6, honeypots, air gapped networks, data encryption techniques and cloud computing security were discussed.

One of the topics elaborated upon was the IPv6 protocol and its impact on overall cyber security wherein the general expectations tend to be very high. Referring to the ISO-OSI layering, IPv6 is just a layer 3 protocol; however, it is the main protocol responsible for addressing the systems in the internet and transporting the payload to the systems. It will introduce encryption on the network layer, which is good for confidentiality and integrity, but at the same time the encryption makes it difficult to scan network traffic for malware targeting the upper layers. The IPv6 is not a silver bullet which will help to solve the cyber defence problems of the future, because it will also introduce new vulnerabilities and new threats targeting those vulnerabilities. As IPv4 and IPv6 will be running in parallel for a while, there will be a double attack surface on the networking layer.

Another double edged sword is related to DPI. This technology can be used for very different purposes. It can be used for internet surveillance by repressive regimes or for finding malware from upper layers' data. Independent of the purpose for which the DPI is performed, it consumes lots of processing power compared to switching, routing or simple packet filtering.

Honeypots provide very useful additional information about potential attackers and their techniques. They can be considered a last level in the defence-in-depth hierarchy. At the same time the analysis of the collected data requires lots of resources and skilled experts.

Encryption, in general, is a very powerful tool if implemented properly. Besides basic principles like using strong passwords with strong encryption algorithms, there are several on-going discussions related to possible backdoors and to secure coding and implementation of the encryption software and to the entire cryptosystem.

'Defence in depth' is the approach to cyber defence where several defence technologies are implemented in succession, such that when one layer of defence fails others will still keep the hackers at bay. This chapter has covered several devices, starting with ACL configured on network switches and routers, moving on to firewalls, and ending with IDS, IPS systems and honeypots.

Summarising this chapter, it becomes clear that there are several controversial aspects and opinions with regard to technical defence methods, tools, techniques and effects in cyber defence. There will be no absolute security and, most probably, new technologies will be unable to change the attack and defence balance significantly, as new technologies also tend to introduce a new attack surface.

References

[1] International Organisation for Standardization, 'Information technology -- Security techniques -- Information security management systems -- Requirements,' 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534.

[2] International Organisation for standardization, 'Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model,' 1994. [Online]. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip.

[3] National Institute of Standards and Technology, 'Guide to Intrusion Detection and Prevention Systems (IDPS),' 2007. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[4] T. Boyles, 'CCNA Security Study Guide: Exam 640-553,' John Wiley and Sons, 2010.

[5] V. Mattord, Principles of Information Security. Course Technology, 2008, pp. 290-301.

[6] Department of Homeland Security, Federal Bureau of Investigation, 'DHS-FBI Bulletins Identifying IP Addresses, Hostnames Associated With Malicious Cyber Activity Against the U.S. Government,' 2013. [Online]. Available: http://publicintelligence.net/nccic-malware-ips/.

[7] C. Parsons, 'Is Iran Now Actually Using Deep Packet Inspection?,' 2011. [Online]. Available: http://www.christopher-parsons.com/is-iran-now-actually-using-deep-packet-inspection/.

[8] A. Soldatov and I. Borogan, 'The Kremlin's New Internet Surveillance Plan Goes Live Today,' 2012. [Online]. Available: http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/.

[9] Reporters Without Borders, 'China,' [Online]. Available: http://surveillance.rsf.org/en/china/.

[10] J. Bamford, 'The NSA Is Building the Country's Biggest Spy Center (Watch What You Say),' 2012. [Online]. Available: http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/.

[11] M. Coward, 'Encryption: will it be the death of DPI?,' [Online]. Available: http://www.telecoms.com/39718/encryption-will-it-be-the-death-of-dpi/.

[12] C.-C. Wu, K.-T. Chen, Y.-C. Chang and C.-L. Lei, 'Detecting VoIP Traffic Based on Human Conversation Patterns,' 2013. [Online]. Available: http://www.iis.sinica.edu.tw/~swc/pub/voip_traffic_detection.html.

[13] Washington Post, 'NSA slides explain the PRISM data-collection program,' 2013. [Online]. Available: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[14] ENISA, 'Proactive Detection of Security Incidents, Honeypots,' 2012. [Online]. Available: http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots.

[15] The Internet Engineering Task Force (IETF), 'Internet Security Glossary, Version 2,' 2007. [Online]. Available: http://tools.ietf.org/html/rfc4949.

[16] D. Terdiman, 'Stuxnet delivered to Iranian nuclear plant on thumb drive,' 2012. [Online]. Available: http://news.cnet.com/8301-13772_3-57413329-52/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/.

[17] C. Florent, 'Security Issues with DNS,' 2003. [Online]. Available: http://www.sans.org/reading-room/whitepapers/dns/security-issues-dns-1069?show=security-issues-dns-1069.

[18] K. Hickey, 'Dark cloud: Study finds security risks in virtualization,' 2010. [Online]. Available: http://gcn.com/Articles/2010/03/18/dark-cloud-security.aspx.

[19] M. Censer, 'Amazon Web Services, IBM battle over high-profile CIA cloud contract,' Washington Post, 2013. [Online]. Available: http://articles.washingtonpost.com/2013-09-01/business/41670836_1_amazon-web-services-cloud-computing-federal-agencies.

[20] The Internet Engineering Task Force (IETF), 'INTERNET PROTOCOL, PROTOCOL SPECIFICATION,' 1981. [Online]. Available: http://www.ietf.org/rfc/rfc791.txt.

[21] International Telecommunication Union, 'ICT Facts and Figures,' 2013. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

[22] Cisco, 'Connections Counter: The Internet of Everything in Motion,' 2013. [Online]. Available: http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342.

[23] Google, 'IPv6 Statistics,' 2013. [Online]. Available: http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption.

[24] B. Schneier, 'Cryptanalysis of SHA-1,' 2005. [Online]. Available: https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html.

[25] European Network of Excellence in Cryptology II, 'ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012),' 2012. [Online]. Available: http://www.ecrypt.eu.org/documents/D.SPA.20.pdf.

[26] SciEngines, 'Break DES in less than a single day,' [Online]. Available: http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html.

[27] M. Buchanan, 'How the N.S.A. Cracked the Web,' 2013. [Online]. Available: http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html.

[28] United States of America, National Security Agency, 'Encrypting Files with WinZip®,' [Online]. Available: http://www.nsa.gov/ia/_files/factsheets/I735-002-08.pdf.

[29] A. Apvrille, 'NSA's (and GCHQ) Decryption Capabilities: Truth and Lies' 2013. [Online]. Available: http://blog.fortinet.com/NSA-s--and-GCHQ--Decryption-Capabilities--Truth-and-Lies/.

[30] J. Cowie, 'Could It Happen In Your Country?,' 2012. [Online]. Available: http://www.renesys.com/2012/11/could-it-happen-in-your-countr/.

[31] M. Fischer, 'The three big questions on Syria's Internet blackout,' Washington Post, 2012. [Online]. Available: http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/29/the-three-big-questions-on-syrias-internet-blackout/.

[32] National Institute of Standards and Technology, 'Guide for Applying the Risk Management Framework to Federal Information Systems,' 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[33] Informationstechnik, Bundesamt für Sicherheit in der, 'IT-Grundschutz,' 2013. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

[34] Riigi Infosüsteemi Amet, 'ISKE juhendid ja materjalid,' 2011. [Online]. Available: https://www.ria.ee/iske-dokumendid/.

*Markus Maybaum**

Technical Methods, Techniques, Tools and Effects of Cyber Operations

1. Introduction

State actors' activities in cyberspace do not focus solely on information technology (IT) security and cyber defence scenarios. Bodies of different State entities have found cyberspace to be a new domain of engagement within the scope of public authority activity. State authorities such as the police, the intelligence services and the military nowadays routinely operate in cyberspace to fulfil their duties: active forensics on suspicious systems as well as intelligence or even military peace time operations in cyberspace have become reality. These activities, summarised under the term 'cyber operations', have one thing in common: breaking into foreign IT systems to extract or modify data, to change the system configuration[1] or to take down the entire system. To put it another way: it is about hacking. Hackers hack; this is more or less commonly known, but does that mean that State cyber operations are conducted by hackers? Or is there a difference between a State actor conducting cyber operations and other hackers? No less important is the question of why hacking is at all possible – which is key to understanding methods of cyber operations. This will be explained by reference to an abstract model for cyber operations which will be introduced in this chapter. Based on this model, the methods of a cyber operation will be explained in seven subsequent stages. For each stage, tools and techniques are introduced with a focus on State actors' use, and these are distinguished from malicious actors.

There is no commonly agreed definition of the term 'hacker' and simply searching the internet for a definition will result in hundreds of suggestions.[2] Asking the hacker community for a definition will result in a different picture: they mostly see themselves as 'clever programmers'. The *New Hackers' Dictionary*[3] provides a list of characteristics that describe a hacker. Hackers:

- enjoy learning the details of a programming language or system;
- enjoy actually doing the programming rather than just theorising about it;

* This chapter is written for a non-technical audience only. All information used is derived from open sources. The chapter represents the personal opinion of the author and should not be attributed to any organisation with which he is affiliated.

1 A change of the system configuration may include the deletion of files and/or services as well as blocking or taking down the entire system.

2 B. Haryey, (1985). *What is a Hacker?* [Online]. Available: http://www.cs.berkeley.edu/~bh/hacker.html.

3 E.S. Raymond, 1996, *The New Hacker's Dictionary*, 3rd ed., Cambridge, MA: MIT Press.

- are capable of appreciating someone else's hacking;
- pick up programming quickly; or
- are experts at a particular programming language or system.

Surprisingly, this definition of hackers does not refer at all to any scientific qualification or education. In fact, many IT officials say that becoming a really good hacker is a matter of talent, so hacking is more of an art than a science. The media uses the word 'hacker' to describe someone who attempts to break into IT systems without their owner's consent, usually referring to a category of people that does this for malicious purposes: juvenile delinquents, criminals or even terrorists. This group of people – often also referred to as so-called *black hat* hackers – uses their proficient technical knowledge for personal or financial gain, or is sometimes motivated by political or religious ideology. Less frequently, there is noise about the category of people hacking for non-malicious reasons – so-called *grey hat* hackers – whose intention is at the 'make-the-world-a-better-place' level: their attempts to break into IT systems are motivated by the will to hunt malware (developers) and spammers, or they are simply testing potential vulnerabilities. When it comes to the so-called *white hat* hackers, people being tasked to break into systems with the permission of the owner (penetration testers, professional security researchers, etc.) or performing cyber operations for States who are entitled to operate in cyberspace legally, there is mostly silence, and for good reason: State actors legally breaking into foreign IT systems is of course hacking, but is only rarely recognised as such in public opinion due to the lack of malicious intent. Thus, different actors are being driven by different motivations, but with one common goal: intrusion into foreign systems. Therefore, when explaining tools, techniques and effects in this chapter, the cyber actors[4] or other hackers will be referred to using the term 'intruder'. If different intruders' motivations imply different behaviour within the discussed method, the type of intruder will be defined. When examples of commonly-used tools will be given, the use of these examples should not be misunderstood as endorsement or suggestion of preferences, or of evaluation of the quality of the tool; they are just meant as examples of tools capable of solving problems at a specific stage of a cyber operation. For any tool mentioned in this article there are alternate tools offering the same or similar functionality, making them equally suitable for the intended effect.

2. Hacking – *Mise-En-Scène* in Seven Stages

How does hacking work? Unfortunately, this question cannot be answered within one or two simple sentences. There is no recipe or check list with which successful hacking could be explained or trained. Hacking is of course taught at universities as well as within the scope of IT security education, and the cyber domain (cyberspace) has been identified as a fifth new operational domain where cyber activities between State actors

4 This term is used for State actors performing cyber operations.

have been seen. The industry employs penetration testers to check their cyber security against cyber crime and espionage. It is essential to know how hacking works in order to defend against these threats effectively, and for a State to make use of suitable tools and techniques within the parameters of law.

In order to understand how hacking works, it is first of all essential to understand why hacking works at all – and the answer this time is simple: it works, because the hacked systems' security is (or was) too weak. This is again easy to explain since there is not much secrecy around the fact that there is nothing like 100% security in IT due to a variety of reasons, as outlined below.

Limited resources in system design and development of systems:

IT projects nowadays have to be calculated competitively, which simply limits the available budget for extended security tests within system developments. One could also say, a little provocatively perhaps, that parts of the security testing nowadays are done by the regular users, and identified bugs are patched once they have been found during the regular use of the system. Unfortunately, some of these 'tests' are done by hackers; what is more, groups of hackers race to be the first to find the security problems. Such security problems can be vulnerabilities caused by programming mistakes or design errors, or simply system misconfigurations.

Weak standard configurations:

Referring back to the problem of misconfiguration, standard configurations of systems can cause severe security issues. A major issue for a long time has been the use of so-called standard passwords: a commercial off-the-shelf (COTS) product is always sold and delivered with the same system administration passwords, and the application does not force the user to change it during installation. This is an open invitation for every hacker. Keeping standard installation directories and standard system settings also helps hackers to predict file directory structures or system registry settings. Standard settings in COTS products only rarely have a strong focus on system security.

User mistakes and lacking awareness:

Even if systems are designed in a very secure manner and have been properly installed and securely configured, mistakes by users or inexperienced system administrators remain a permanent risk to the security of systems. Security breaches may happen in various ways: the importation of malicious software, the disclosure of sensitive information, or even attempts to improve system security, which may have the opposite effect if done incorrectly. The fact that a list of possible security breaches by people would be very long illustrates the variety of threats arising from them. Hackers have and use this knowledge.

A strategy to hack a system can be derived from knowing that hacking is about getting information about a target system in cyberspace, finding clever ways to exploit its vulnerabilities, making use of its misconfigurations or taking profit from its users. Since

the talent or intuition of a hacker cannot be expressed in a scientific way, this chapter will focus on best-practice models designed for the white hat hacker community. A model for cyber actors' engagement suggested and used by the United States Department of Defense (US DoD)[5] in the military domain will be used to illustrate stages of a cyber operation (see Figure 1). There are other models describing cyber operations or the generic process of hacking at a more abstract level, as well as models that refine the model to nine or more stages. The US DOD Cyber Operation Model – often also referred to as the so-called *Cyber Kill Chain* (CKC) – shall be used in this chapter since it is used by a majority of cyber actors and is useful in explaining the necessary steps for successful acting in cyberspace at a fine-grain level to a non-technical audience without getting lost in technical details.

Figure 1. Cyber Kill Chain Model.[6]

Cyber actors are trained to use their equipment, methods and techniques at the tactical, operational and strategic levels. Unlike a designated cyber defender, cyber actors need to be capable of intruding into other systems and acting to fulfil their mandate as well as acting within the scope of self-defence. This intrusion into systems, which basically describes the process of hacking, is referred to as a *cyber attack*. NATO defines cyber attacks as 'actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves,'[7] and most scientific and legal definitions define cyber attacks in this or a similar way. Thus, since a cyber attack is, by definition, a type of computer operation that seeks to disrupt, deny, degrade, or destroy information, computers or computer networks, the term 'cyber attack' will be used as a synonym for hacking in the context of this chapter and must NOT be misunderstood as an indication for any non-peacetime State activity.

5 E.M. Hutchins, M. J. Cloppert, and R.M. Amin, (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,* paper presented at the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, 17–18 March 2011. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

6 I. Lachow, 2013, Active Cyber Defence – A Framework for Policymakers, Center for a New American Security (CNAS) Policy Brief. Available: http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

7 NATO Standardization Agency, *NATO Glossary of Terms and Definitions* (AAP-6) at 2-C-12, 2012.

Cyber attacks can be analysed in a number of sequential steps, starting with the preparation stage and ending with exploitation, command and control, or attack persistency, depending on the objectives of the mission. These stages have been modelled in life-cycles serving as a framework for any cyber operation. The CKC model defines the phases of such an operation to be reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and action. These stages will be used to describe the sequence of activities, and to introduce tools and techniques to be used within each stage to match all the defined objectives, which are essential to proceed to the next stage in a cyber attack against an IT system.

Within a cyber operation, a distinction is made between the preparation for and the conduct of cyber attacks. This chapter will focus on means and methods of hackers within the so-called *Cyber Engagement Zone*, which is the cyberspace equivalent of a battlefield in the real world and which is the system to be hacked. Before any cyber attacks against a target can be launched, the first two steps of planning and preparation, reconnaissance and weaponisation, need to be carefully considered since they prepare the grounds for the success of any cyber operation. The following sections will explore each of these phases in detail.

2.1 Reconnaissance – Get Information about Your Target

As in any operation, cyber operations need to be planned based on relevant and reliable[8] information about the operation's targets; information important to the decision making process must be gathered, and its integrity, authenticity and correctness assured. This implies the need to gather information about the target in the best possible manner to be able to derive a solid situational picture, on which basis different courses of action can be assessed. It also requires reliable information about the status of one's own capabilities and available resources. The process of collecting this information is called *footprinting*: collection of information available from open sources or provided by services is known as *passive footprinting,* while *active footprinting* refers to one's own actions within the cyber operation to obtain missing information, and is analogous to battlefield reconnaissance.

The most convenient way to gather the required information is open source intelligence (OSINT). OSINT covers the entire range of publicly available information about the operation's target and therefore is not an easy task. The challenge starts with finding open-source resources, using tools and intelligence sites already available on the internet, and filtering the information needed for the intended operation. Using OSINT for reconnaissance purposes must therefore be seen as a very important first step which should not only be considered in the operation's planning stage, but also in any subsequent stage of the cyber operation as soon as new information is derived which

8 The integrity, authenticity and correctness of the information need to be assured.

updates the situational picture, and which might influence decision making and the action of current operations.[9]

Within the scope of cyber operations, information about cyberspace structure provided by the Internet Cooperation for Assigned Names and Numbers (ICANN)[10], its subordinated Regional Internet Registries (RIRs), and the Internet Assigned Numbers Authority (IANA)[11] is required. This is evaluated with further detailed information which can be retrieved from WHOIS and Domain Name System (DNS) servers. WHOIS is an application-level protocol – defined in the Internet Engineering Task Force (IETF) 'Request for Comments' (RFC)[12] 3912 – providing domain, Autonomous System (AS) and Internet Protocol (IP) information; DNS is a service to resolve IP addresses from the human-readable Uniform Resource Locator (URL) format. Very often, further information can be found by simply accessing the target's offered services,[13] or by using social media. Social networks have been identified as another primary source of information in the process of intelligence gathering. Social network information can be OSINT information or protected information, access to which requires membership of the social network or approval by the information owner. This can be circumvented by operational actions taken, such as providing false information or using a fake identity, or by information or identity theft – at least from the technical perspective.

Apart from open sources, classified information provided by governmental or military intelligence agencies – if available – can be used to update the situational picture. State actors usually have access to classified information and use this for the assessment of sensor data. In comparison with OSINT, the access and evaluation is easier since intelligence agencies tend to organise their information in accordance with their users' needs. Intelligence agencies also keep their classified information updated, so the information gathered from them can be expected to be up-to-date. Sometimes even real-time information is available, if there is direct access to such intelligence databases. Classified information should therefore be used in addition to OSINT whenever possible.

Since all that information will require verification and updates, one's own means and methods of reconnaissance have to be applied. To be able to operate in cyberspace, the overall requirement is the accessibility of the cyber engagement zone and the targets to the intruders, which means that intruders must be able to find the targets and generate an effect on them. Finding a target is straightforward as long as it is directly connected to the internet and thus is registered with its internet service provider (ISP) and its IP

9 For a good overview on OSINT tools and resources see: R. Hock. (2013 September 13). *Internet Tools and Resources for Open Source Intelligence* [Online]. Available: http://www.onstrat.com/osint/.

10 See internet portal of ICANN. Available: http://www.icann.org.

11 See internet portal of IANA. Available: http://www.iana.org.

12 Defined in RFC 1034/1035. RFCs are agreed technical standards published by the Internet Engineering Task Force (IETF). See internet portal of the IEFT. Available: http://www.ietf.org/rfc.html.

13 Such a service is, e.g., a hosted web-site.

address information, available through internet information services. Unfortunately, many potential targets are not exposed directly to the internet, but are protected by gateways, firewalls and Intrusion Prevention Systems (IPS). These are known as *fenced systems*. To find these systems, cyber operations are often targeted not only against single systems, but against entire clusters or collaborating computer networks. If a cyber operation is explicitly targeted against a single system, independent neutral systems might have to be affected in order to reach the target, which must be seen as a legal challenge if the owner's consent cannot be achieved.

Active footprinting will therefore always start with *scanning* and *fingerprinting* systems that can be directly reached through the internet; if fenced systems need to be scanned, this will be done as soon as a way through the fence has been found. Scanning systems usually starts with a port scan. Ports are the communication connections into and out of a computer system. A port can be open, filtered or closed. If a port is closed or filtered, communication through that port is disabled, so it cannot be used within the intended cyber operation. If a port is open, it can possibly be used, but further investigation is required.

Each port provides or accepts a specific service which is offered in a well-defined data format (protocol). There is a set of ports (so-called *well-known-ports*) which – with a few exceptions – offer standard services that are published by the IETF in their RFCs, but most ports are so-called private ports. Some of those private ports are also associated with widely known services since certain COTS products use them by default, but there is no guarantee. Different COTS products might use the same port or ports could have been modified manually. In addition, there are millions of non-COTS products in cyberspace without any port documentation, as well as manually-opened connections where no information about the intended or actual use is available. So within the process of reconnaissance, all open ports have to be verified, including the most commonly used and well-known ports. This is because actors with malicious intent tend to change ports to confuse analysts and to slow down counter operations. Therefore, as a second step within active footprinting, port scans are always followed by protocol probes to verify whether or not the expected service is indeed offered at the found port. Protocol probes first try to establish a connection to a port using the expected protocol, if well-known or associated. In case of success, a service might have been identified, but a service can also be simulated by malicious actors to confuse the analyst. In any case, all known protocols have to be tested at this port. This will either result in a positive service identification or in failure. If no protocol can be identified for a port, activities at this port are limited to traffic monitoring, itself a method of intelligence gathering, and to service denial attacks.

Once services have been identified by protocol probes, more detailed information about the scanned system can be retrieved. The aim of this third step of active footprinting is to gather detailed information about the configuration of the scanned system and thus

derive a network fingerprint. Certain port combinations or services can help predict the operating system running on that machine, and communication tests (so-called *banner grabbing*) towards those services can yield detailed information about software products and versions installed. All that information must be analysed carefully in order to successfully prepare the intended cyber attack against the target.

If the target is a network, the network connections within that target must also be explored. This is achieved by *tracerouting*: step by step, possible routes from the own systems to the target are tested, and a fine-grain network picture is derived. This network cartography can be done from different systems which will refine the picture.

Also neighbouring systems[14] in the network can be scanned and tracerouted to refine the picture and to investigate for suspicious activities or fingerprint (suspicious activities shall be understood as any action that could be interpreted as malicious, and suspicious fingerprints are found on a system which has the same network fingerprint as systems that have already been identified as malicious). During the entire cyber operation, all this information must be updated regularly since owners of targets can be assumed to use modern techniques to strengthen their systems' resilience, including making changes to network fingerprints and available services at ports. This is especially important if such changes are monitored in very short time intervals, otherwise successful weaponisation – as described in the following section – is almost impossible.

The scanning of networks can be done manually with tools provided by the operating systems, but nowadays, it is usually automated. Networks are usually explored by pinging target systems[15] based on technologies of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP). Unfortunately, systems can be configured to block ICMP functions, so pinging does not always provide correct results. In a worst case scenario, all ports of a target must be tested without knowing if the target can be reached at all, which is a very big task. Port scans and port probes can be done by port-scanners. Modern port-scanners can scan entire network segments without any human interaction, including port probes of the well-known ports and protocols. A very common and widely used tool for port-scans is, for example, NMAP.[16] This tool is freely available through the internet and offers all the functionality for port-scanning as described. To a certain extent, it also offers port probes and operating system recognition functionalities. For proprietary protocols and extended network fingerprinting additional human effort is required. Especially for unknown communication formats, manual investigation will always be required. In this case, traffic needs to be monitored and data formats recognised

14 The term 'neighbouring systems' is to be understood in a technical sense, for example, as systems being in the same network segment.

15 For a very good introduction into pinging techniques, see R. Natarajan (30 November 2009) *Ping Tutorial: 15 effective ping Command Examples,* The Geek Stuff [Online]. Available: http://urli.st/3ur-The-Geek-Stuff/hU-Ping-Tutorial-15-Effective-Ping-Command-Examples.

16 See internet portal of the NMAP Security Scanner. Available: http://www.nmap.org.

and re-engineered. Traffic monitoring is done with the help of network traffic scanners and network protocol analysers such as tcpdump[17] or Wireshark[18]; the latter has more or less become the standard tool for this purpose. For the re-engineering of proprietary network traffic, IP packets must be built and tested manually or batch routines written. The variety of packet builders freely available on the internet is remarkable.[19] Packet builders are available for any operating system, command line or graphic user interface, and they all come with different additional functionality for research and analysis as well as for penetration and professional use. Besides building packets, captured packets from recorded network traffic can be used either by simply resubmitting them or by modifying information to explore the protocol structure. If during this re-engineering or any other phase of active footprinting different behaviour is found when using the own IP address for analysis, third party systems can (or even must) be used to get the required data (with or without the consent of the rightful owner).

As a result of all these reconnaissance activities, a detailed situational picture of the target is derived and continuously updated during the upcoming stages of the cyber operation. Once an intruder gains access to the target system, the picture is enriched by the information found on the target or on other intermediate systems being used to break into the target. Situational pictures are usually kept in databases designed for that purpose and tools are designed to feed their information directly into these databases to update the picture in real-time.

2.2 Weaponise – Prepare to Break the Shields

Intruders need to be equipped and trained to be able to engage in cyberspace. Once a target has been identified in cyberspace, a cyber situational picture has been derived and a network fingerprint has been made, the most challenging part of the mission preparation is to find suitable cyber means to take effect on the target. Such means of cyber activities in this context are all IT hardware and software items as well as other systems capable of taking effect in cyberspace, such as computer programs or malicious software. A great variety of terms has been used recently to describe those means of cyber activity, mostly without giving a definition or even an explanation of the exact meaning of the term. For non-technical users, terms like ‘hacking tools’, ‘exploits’, ‘malware’ or even ‘cyber weapons’ are likely to be misunderstood and are hard to distinguish from other tools which lack a malicious character or are by design capable of dual use. Due to a lack of common definitions, and since for the purpose of this chapter an expert-level understanding of all the technical details is not required, all means of cyber activities being used within the scope of cyber operations shall be referred to by

17 Included in any Linux distribution as part of the operating system.

18 See the internet portal of Wireshark. Available: http://www.wireshark.org.

19 For a list of examples see a Wikipedia collection. Available: http://en.wikipedia.org/wiki/Packet_generator.

the term 'cyber tool'. A cyber tool can be a cyber weapon especially designed to break into foreign systems and perform malicious actions, or it can be a regular tool which is used within cyber operations as well as for regular system operations or maintenance.

From a technical perspective, a cyber operation can therefore also be understood as a well-planned sequence of cyber tool engagements to achieve a pre-defined goal. For this, cyber tools being used to break into foreign systems must be customised to their target, and they need to be of high precision: one bit set wrong in such a cyber tool can render it useless. Thus, each cyber tool has to be individually prepared and tested for use against its intended target based on the findings of the reconnaissance phase. This means that the type of target determines the cyber tool of choice. In cyberspace, there are 3 categories of targets:

1. Unprotected targets – no protection mechanisms exist or existing protection mechanisms of the target are not in force.
2. Regularly protected targets – existing protection mechanisms of the target are being used and COTS IT security products such as virus-scanners or firewalls have been installed.
3. Specially protected targets – in addition to standard protection mechanisms and COTS IT security, the target has been hardened by individual intrusion detection and intrusion prevention systems (IDS/IPS) and is being monitored by specialised security information and event management systems (SIEMS).

Whereas for successful intrusions into unprotected systems a cyber tool might not be needed at all if the intended action can be achieved using simple tools one can find on the internet, regular protected systems raise the level of difficulty dramatically. In terms of kinetic weapons, if the successful intrusion into a regular protected target requires the cyber equivalent of a crow bar, a defended target will require the cyber equivalent of a high-explosive anti-tank (HEAT) missile[20] or even a bunker buster. Continuing with these metaphors, it becomes clear that the design of a cyber tool requires two major components: an armour-piercing penetrator to break the system's protection and a payload causing the intended effect on the target. The penetrator of a cyber tool is called an 'exploit'. This usually consists of a privilege-escalating machine code injected into data which is submitted to the target system. Exploits are very clever pieces of software that use vulnerabilities, so the more a system is hardened, the more difficult it is to crack the virtual bunker. But it is possible. Sophisticated exploits contain multiple elements not only to break the shields at the vulnerable point, but also to modify the used vulnerabilities on the target system. Some very sophisticated exploits even work with different operating systems, especially if during the reconnaissance phase the exact operating system version has not been identified. Payloads usually include information

20 This metaphor is comparing the protection mechanisms of the target with the armour of a tank that needs to be cracked.

(data and software) which is required to achieve the intended manipulation of the target system; they will be described in the installation phase of the cyber operation (see section 2.5). If no further action on the target is planned, a payload might be not required at all.

Weaponisation is the process of identifying suitable cyber tools which would enable a successful cyber attack on a system. Since exploits use identified vulnerabilities, misconfigurations or user mistakes to gain access to targets, identifying suitable vulnerabilities or misconfigurations is the first step in the weaponisation phase. The network fingerprint and the cyber situational picture as derived from the reconnaissance phase provide valuable information for that: identified services can be checked for known vulnerabilities, particularly if detailed version or 'build information' can be retrieved by banner grabbing. Computer Emergency Response Teams as well as the IT security industry offer Common Vulnerability and Exposure (CVE) databases that list all known vulnerabilities reported by security analysts or researchers. Since these databases are quite complex, a special class of software known as a vulnerability scanner has been invented to automate the vulnerability detection process. Vulnerability scanners often use built-in functionality to perform target system reconnaissance and are used by intruders and penetration testers to analyse a system's attack surface. There is no dedicated standard tool in the area of vulnerability scanners;[21] in media as well as literature NESSUS[22] is often referred to as the tool of choice when performing a vulnerability scan since its false-positive rate[23] is low. False-positives slow down the weaponisation process because time and resources are invested into finding or creating a cyber tool which ultimately will not work on the target – therefore it is important to keep this rate as low as possible.

The design of cyber tools used to gain access to the target system is usually based on exploits that make use of a vulnerability to alter the program flow of the target system in order to execute an injected code granting full system access to the intruder. These tools and codes can be simple scripts, cleverly modified software, code injected into data, or highly sophisticated malware. A cyber operation will often also consist of a combination of techniques being applied in sequence. Very sophisticated cyber operations foresee backup cyber tools for different versions of operating systems with different patch levels,[24] and they use so-called 0-day exploits. The latter make use of identified vulnerabilities that have been found by security researchers or the hacker communities, but have not yet been published in the vulnerability databases, which implies that there is no patch for this vulnerability.

21 See Sectools internet portal. Available: http://sectools.org/tag/vuln-scanners/.

22 See Nessus internet portal. Available: http://www.tenable.com/products/nessus.

23 A false-positive is a found vulnerability which in reality is none.

24 A patch level describes the state of a system in terms of fixed known vulnerabilities: a patch fixes a vulnerability; keeping a system at its latest patch level minimises the risk of being exploited.

Weaponisation also differs a lot depending on the type of intruder. Whereas State actors and other entitled intruders have to care about the used cyber tools and the need to avoid conflict with the law, malicious hackers do not care too much since they are in conflict with the law anyway and flout licence agreements, copyright and data privacy regulations to get what they want – options not necessarily available to State actors. The biggest obstacle for governmental cyber actors are licence agreements. State actors are limited to the lawful use of software and tools, and most software products available on the markets prohibit their use for offensive purposes, which a cyber operation certainly is. Therefore, lawful cyber operations are very much dependent on the in-house development of cyber tools, whereas malicious intruders just misuse available products. They also modify existing products to convert them into cyber tools, which cannot be done by a white hat actor without the rightful owner's consent.

The development of a cyber tool requires knowledge, time, resources and a test stage. Since State actors are dependent on in-house-developments, 0-day exploits have been found to be valuable to hacker communities. Whereas in the past the black hat communities used their findings to hack and act, recently, a tendency towards a change of attitude can be recognised: 0-day exploits are now sold to the IT security industry as well as to State actors who very much rely on them to create cyber tools they need for cyber operations they are tasked to conduct. Black hat communities also sell user credentials they successfully steal from targets. Unfortunately, the use of stolen identities and fake identities to gain access to systems is also very limited for State actors due to legal implications, whereas malicious actors do not care. The same applies to the use of illegal tools and software: whereas malicious intruders use this kind of software, particularly to hide malicious cyber tools, authorised actors cannot. Regrettably, there is no guarantee that all State actors always act in accordance with their given laws. Therefore, recognising a cyber attack as being conducted with illegal cyber tools does not in general allow the conclusion that non-State actors are involved, but it can be an indication.

With regard to the selection of a specific cyber tool, the first choice is always a known vulnerability which is published and for which exploits have already been developed. Due to the poor patch levels of many systems, these kinds of cyber attacks are successful more often than one might expect. New exploits are published on the internet almost on a daily basis, so the intruders' chances of finding a suitable tool or exploit are high. By using publicly available tools, intruders can save their financial means and resources for the development of 0-day-exploit-based cyber tools. If the product of choice is or even needs to be based on a 0-day exploit, the intended operation becomes time critical since its success is very much dependent on the confidentiality regarding the vulnerability involved. Once this vulnerability is published, it will usually be quickly patched by the vendor which will make the cyber tool useless. Consequently, there is a race between intruders developing cyber tools and the IT security industry conducting research on vulnerabilities.

Weaponisation is also an iterative process since updated information from the situational picture may highlight a need to change or modify the cyber tool of choice. Without appropriate cyber tools, access to systems can only be achieved by taking advantage of misconfigurations or user mistakes. If a target system is not properly protected and cyber tools are not needed at all, intruders can start to manipulate the target system directly. Otherwise, once a cyber tool has been tested successfully,[25] the delivery of the tool to the target system needs to be planned.[26]

2.3 Delivery – Get the Tools to the Target

The delivery phase of a cyber operation describes the transfer of a cyber tool to the target system. Depending on the nature of the cyber tools, different approaches to delivery can be chosen. Again, State actors are more limited since they should ensure that intended manipulations only affect the target system and no side effects occur, whereas malicious hackers will not care too much, and may even use third party systems as proxies to launch their cyber attacks.

In case of user mistakes or misconfigurations, the delivery of the payload can be very simple: it may be that, due to missing or incorrect access control modifications on the target system, delivery is possible without any further action by the intruder and a payload can just be uploaded and installed. This, of course, will only be possible in exceptional cases. Generally, access rights need to be gained first or access control mechanisms need to be circumvented. Gaining access rights can be achieved in different ways, and the method of choice depends on the information gathered about the target system during the reconnaissance phase. The easiest solution to the challenge would be the use of target system user credentials at the administrator level. In that case, the system is 'owned'[27] insomuch as the intruder can carry out any modification to the system, including the installation and deletion of software and data, as he chooses. Once the credentials have been used to log on and the logon has been granted,[28] no further exploitation of the target system is required.

If user credentials at non-administrator level are used, this may not suffice to deliver the payload successfully to the target system. In that case, the available user credentials with minor privileges can be used to gain access to the system and – after successfully having logged on – to raise the privileges using other cyber tools made available in the weaponisation phase. If no cyber tools are available at that stage, a step back to reconnaissance might be required to evaluate the target system information accessible with the user credentials used to log on, and to consider new techniques to escalate

25 A test is not always possible and reasonable, thus not all targets can be emulated to test the cyber tool.

26 The requirements of the cyber tool delivery can have influence on the tools' development.

27 Hackers use this term to describe full access rights to a hacked system.

28 Awareness of user credentials disclosure often results in the deletion or disabling of the referred user account.

the privileges. If this is not successful, a different way to deliver the payload to the system needs to be considered. Delivering a payload to a target system without suitable permissions on the target system can be achieved in two ways: making a user with sufficient access rights install the payload for the intruder or exploiting the target system and installing the payload without logging onto the system.

There are different ways to make users of a target system help the intruder install a payload. The easiest is obvious and should be well known: mail the payload to a target system user as an email attachment and make him install it on the system. Since a cautious user will not do that voluntarily with unknown mails, there are numerous options to manipulate him into doing so. The payload can be inserted into other files which the user may want or even need to install on his system – updates for software for example. Indeed, some very clever hackers managed to infect security updates with payloads, and so in patching their systems, which normally helps to protect against cyber attacks, users got infected. This is a very sophisticated approach which requires very detailed knowledge about the configuration of the target systems as well as manipulation of the update procedures. Much easier to implement and mostly also successful is the use of 'social engineering' in combination with emails: who would suspect an email from a friend using a familiar language and style of writing and even a familiar attachment name? This is what sophisticated hackers do: analyse contacts and recorded email exchanges between users on the target system and use this information to send a malicious attachment to a user in the name of a good friend or business contact. The rate of successful cyber attacks using this technique is high and it opens 'backdoors' for the intruders, so that they own the system without the owners' and rightful users' knowledge. However, since such malicious attachments to emails are likely to be detected by anti-virus systems, a change of strategy can be seen. Recently, the malicious payload is put onto web servers and a user is misled into downloading it from the internet onto his or her machine. This can be achieved by sending emails with a faked sender's address, including links instead of attachments. Even more sophisticated would be an approach where the users' behaviour on the internet is analysed and the payload is included into some content the user is known to download – if this is predictable and the payload can be placed in such files.[29] Technically, it would be sufficient to redirect the user of the target system to a previously prepared website which is ready to install the payload on the target system when being requested – a so-called *drive-by download*. This technique has especially been seen on a lot of sites offering free games, videos, music, illegal software or adult content. In comparison to targeted cyber attacks within a cyber operation, these sites are designed to infect any visitor. This makes the technique difficult to use for targeted cyber attacks, although it is possible and has been seen recently as well.

29 This could require hacking a third party system if the owner's consent cannot be achieved differently.

Less widely known are cyber attacks carried out within the scope of social networks. Drive-by downloads might occur here as well, and will be more sophisticated than those from emails and malicious websites. Whereas malicious websites can be blacklisted by the IT security community and be recognised by cyber defence systems, content of social media cannot, unless access to the social media network is blocked entirely. Social networks are very commonly used, which means that no cyber security company would include them in a black list. Due to the highly interactive nature of social networks, the content of these websites changes rapidly as does the group of people being exposed to the contents. Therefore, using pattern matching and anomaly detection techniques at web-level are also not very reliable methods when it comes to preventing of malware downloads from social networks. The effects remain the same: the user of a target system uses social media and is manipulated by an intruder into downloading a hidden payload to his or her system, which creates a backdoor for the intruder to get onto the system and own it.

The most difficult and highly sophisticated form of delivery is the delivery by a *service exploit*. If the users of a target system do not 'help' the intruder to install the payload on their system, vulnerable services running on the target system can be used to get the payload in. In general terms, a vulnerable service may allow a user to copy the payload onto the system without any user credentials or security checks. Any service running on a computer can be vulnerable and be misused by intruders, and that's why system administrators normally limit the number of services they offer to a minimum.

The delivery of payloads can be automated. The most common form of automated payload spreading is a computer *virus*. Replication mechanisms designed to copy malicious software have been explored for decades and are improving continuously. Viruses use all the delivery concepts described above and can be designed to be targeted (to attack only a specific system) or to be non-targeted (to infect any system on which it is downloaded). Delivery by service exploits, especially by *worms*, needs to be taken seriously as well. Such malicious software may evolve through networks without any user interaction, and infect entire network segments at internet speed. Worms can carry payloads, too, and may also be targeted or non-targeted, but the most sophisticated way of spreading payloads, either targeted or non-targeted, is by the use of botnets.

Botnets have become a major tool in cyber operations since they automate the process of delivery and, as recently discovered, can do this in a very targeted way. For example, *Operation Red October*, one of the most sophisticated botnet-based operations so far identified, uses different mechanisms to precisely select its targets. This is probably why it remained undetected for more than five years. At present, there is no commonly agreed definition of a botnet, but in this chapter, the definition of Kaspersky Labs, a major player in the IT security industry, shall be used. According to them, 'botnet'

> is the generic name given to any collection of compromised PCs controlled by an attacker remotely. Botnets generally are created by a specific attacker or

> small group of attackers using one piece of malware to infect a large number of machines. The individual PCs that are part of a botnet often are called 'bots' or 'zombies' and there is no minimum size for a group of PCs to be called a botnet. Smaller botnets can be in the hundreds or low thousands of infected machines, while larger ones can run into the millions of PCs. Examples of well-known botnets that have emerged in recent years include Conficker, Zeus, Waledac, Mariposa and Kelihos. A botnet is often discussed as a single entity, however the creators of malware such as Zeus will sell their wares to anyone with the money to pay for them, so there can sometimes be dozens of separate botnets using the same piece of malware operating at one time.[30]

Thus, botnets are first of all cyber tools themselves since they use spreading techniques to deliver cyber tools to target systems. They are able to automate significant parts of cyber operations since they are capable of automating command and control as well as any action to be carried out at the target system, which, in case of a botnet, usually consists primarily of persistent and resilient infection of the target and a malicious mission to perform on the target. These missions might include infecting more targets, information exfiltration, or system modification. Nowadays, botnets are the most efficient tool of choice for the delivery of cyber tools, not only since they work at network speed, but also because attribution back to the intruder is very well disguised. As of today, the origin of the big botnets mentioned by Kaspersky is still unknown, as is that of most of the other botnets so far discovered.

Once a botnet has delivered its cyber tools to the target system, they have been shipped there manually, or the target system user was fooled into downloading them, an exploit must modify the system in a way that allows the execution of a payload, so the cyber operation can continue as intended. This penetration of protection mechanisms, when not based on user credentials, is called vulnerability exploitation.

2.4 Exploitation – Hijacking the Control Flow

Hackers like to see themselves as very smart programmers, and there is good justification for that. When user credentials cannot be used to get administrator or system level access to a target system, clever ways of deviating target systems from their regular program control flow into payload execution must be found during the weaponisation phase. It is essential to understand why exploitation works and why it is at all possible to alter the control flow of a program during its runtime.[31]

---

30 D. Fischer, 2013, *What is a Botnet? (Botnet Definition),* Kasperspy Lab [Online], 25 April. Available: http://blog.kaspersky.com/botnet/.

31 Software is usually executed in a process structure which is protected by the operating system against any external modification.

One of the most important requirements for exploitation is the physical ability to alter the program control flow on the target system. This basically means that a program needs to be executed in a computer's random access memory (RAM); if the memory is read-only, the program flow cannot be altered and an exploitation would not be possible. Modern computer architectures are designed for data and software to share the system's memory.[32] Except for the Basic Input Output Systems (BIOS), needed to boot up a system, all software is copied into RAM before it is executed. Since the available memory used by a program is shared by the program code and the data being processed, the program code can be altered if it is, at least in part, buggy, and data parts of the memory can be accessed and modified in such a clever way that the program control flow can be changed as well.

The easiest way to alter the program control flow is to use so-called *overflow techniques*, for example *buffer overflows*. Buffers are dedicated pieces of memory used to store user input data during program execution. If user input is accepted during the execution of a subroutine within the program, it can be stored within a data structure which is called a *stack*. This is very likely, as programmes usually consist of a lot of subroutines that are reused by different parts of the program to keep the code short. A stack is the dedicated piece of memory space assigned to each process of a computer, and regulates subroutine calls. When a program calls a subroutine, it stores required parameters on the stack to provide the subprogram with the data it needs to process. Since a subprogram can be called from many different parts of the program, it needs to know the memory address to return to after the subroutine has finished. This return address is stored on the stack as well as data and buffers for inputs. Normally, all these items 'pushed' onto the stack have a dedicated size, so after the subroutine has finished, the stack can be cleaned up again[33]. The problem why exploitation of the stack worked quite well for a long time was that, unfortunately, a number of software compliers[34] did not check if the user inputs to the system really did fit into the dedicated buffer space being reserved on the stack. Thus, if a user created an input for the program that exceeded in size the dedicated buffer space, the rest of the buffer was overwritten with the rest of the user input as well, including the address to return to after the subroutine has finished. So by cleverly researching the exact length of required user input and replacing the return address on the stack with a memory address pointing to the payload placed on the target system, a program control flow can be altered during runtime. These techniques are called *overflows*; they not only work on a process stack but also on a process heap.[35] So when the subroutine finishes after a successful overflow exploit, the program will return not to the position

32 So-called *von-Neumann architecture*.

33 Otherwise a process would run out of memory quite fast if all subroutine calls would just put things onto it.

34 A program that creates the executable binary containing the program code from a human readable programming language.

35 A 'process heap' is a memory space additionally allocated to a process during program execution.

the subroutine was called from, but to the new address specified in the submitted data. This should be the position of the payload being delivered to the system. A very clever way to place the payload within this kind of exploit was inside the user data being used for the overflow attack itself. For a long time this was easily possible since creative hackers developed payloads which could exploit systems sized significantly less than 100 bytes.[36] For example, shell codes typically start a command shell from which the attacker can issue commands to the target. The shortest shell code (a piece of code providing the attacker a command shell on the target system from which any available command can be executed) on a target system can be accommodated in just 24 bytes of memory space, and even more advanced call-back shell code – connecting back to a remote shell on the intruders' system – requires a few hundred bytes only.

Modern operating systems have protection mechanisms that help to avoid or at least minimise these easy types of exploitation. One of the challenges when trying to develop an overflow exploit is to acquire the knowledge about the exact memory positions of the payload, so the return address of the vulnerable subroutine can be modified accordingly. In older operating systems, this could be easily achieved since – within a process – this address would have been always the same, so the payload address was constant. Modern operating systems provide protection mechanisms to alter the memory layout of a process based on a random value.[37] The challenge is to find out the exact memory location within software during its execution, which is not an easy task, but can be achieved by some very sophisticated programming techniques. Even more challenging are protection mechanisms that define distinctions between different types of memory and do not allow execution of code within stack or heap memory anymore. This raises the level of challenge for intruders to a new dimension, but still does not provide security since intruders can try to compose their payload from parts of the existing code of the program itself and modify subroutine calls accordingly.[38] Without going into too much technical detail, it should have become clear that from the current architecture of systems that execute program code in RAM, only smart intruders can always find a way to deliver a payload and deviate the regular program flow into the payload, if they find a suitable vulnerability. This is almost always possible since entirely correct software that is free of vulnerabilities is too expensive to produce.

Exploiting a vulnerable process does not automatically require system or administrator privileges. Most of the processes running on a system are actually user level processes which do not need the privileged permissions required for a system takeover or the installation of a new functionality on a target system. Priority in vulnerability finding

36 One byte is the equivalent of one character user-input here.

37 So-called *address space layout randomisation* (ASLR).

38 One famous new approach in this field is called *Return-oriented programming* (ROP) – see R. Roemer et. al., *Return-Orientend Programming: Systems, Languages, and Applications* in ACM Trans. Info. & System Security Vol. 15, March 2012 [Online]. Available: http://cseweb.ucsd.edu/~hovav/papers/rbss12.html.

is therefore given to kernel processes and processes running with system rights. If the program control flow of a process with privileged permission can be deviated into payload execution, the payload has system rights and only then can it make any necessary modification to the system. This is what needs to be achieved for the installation of a cyber tool on the target system. The number of processes in operating systems running at system privilege level is continuously increasing with each new operating system version appearing on the market. However, the quality of software has increased as well, so finding vulnerabilities in kernel modules is more difficult. The problems nowadays are third-party tools and COTS software being installed on target systems running at system level and having vulnerabilities that can be exploited. For example, web browsers have long been a primary target for exploitation. Recently, especially vulnerable browser plug-ins have been seen as well as plug-ins with built-in malicious content, often in combine with cleverly designed drive-by payloads and exploits for browsers or their plug-ins during runtime. After installation, these plug-ins open 'backdoors' for intruders, often hiding the malicious communication in regular web traffic. Other vulnerable products have been seen as well, such as instant messengers or voice over IP solutions. Also standard COTS programs such as Microsoft Office have shown to be vulnerable to clever exploits; indeed, modern botnets as seen in *Operation Red October* use MS Word and MS Excel vulnerabilities to exploit the target systems. The more software is identified on the target system during the reconnaissance phase, the more likely exploitable vulnerabilities can be found. In other words, being invulnerable to sophisticated exploitation is unlikely if COTS software is installed on a system. This implies that, except from some rare exceptions, computer systems must generally be considered to be vulnerable to exploits, and the fact that exploits have not been made public does not imply they do not exist or have not been found.

Exploitation can be automated using exploitation tools and frameworks. One of the most common tools in this field is Metasploit,[39] an exploitation framework that offers cyber tools to exploit known vulnerabilities and to combine them with a choice of useful payloads giving remote access to the target system. Officially, Metasploit is a penetration testing tool, is marketed as such, and it offers well-known vulnerability exploits only. However, an intruder can easily add lesser-known or even 0-day exploits and misuse the tool for malicious action. All exploits can be used with a specialised command shell that allows easy customisation to adapt it to the target system specifics. Of course, all exploits can be executed manually as well, e.g., by using script languages or by using vulnerable services with arbitrary data, for example, by entering exploitation data into a web form in order to exploit a web server.

Successful exploitation provides privileged access to the target system without the need to have user credentials granting such access. Exploits are mostly combined with

[39] See internet portal of Metasploit. Available: http://www.metasploit.com/.

payloads that create a communication channel between the intruder and the target system. The modifications done by the exploit are not persistent at this stage; the payload is only stored in the RAM and executed there. To create a permanent backdoor to the target system or to prepare and perform the intended actions, the installation of loaders,[40] access tools or other malicious software is required. Very sophisticated exploits can additionally erase their traces after the payload has been placed. Therefore, manipulations of the program control flow that have been used to exploit the systems can be undone to wipe the intruder's traces. If this is done properly, even professional forensic tools cannot prove the use of an exploit that penetrated the system security. Wiping traces is especially done if 0-day exploits are used, in order to keep them secret and to obfuscate technical attribution. The only way to monitor such modifications are memory images that must be made and analysed on a separate machine, which is a very advanced technique requiring expert knowledge and a lot of resources, and will therefore only be conducted in very exceptional cases.

2.5 Installation – Reside the Payload on the Target

Having successfully exploited a target system, or having gained access to the system due to misconfigurations or user mistakes, the malicious actions intended to be carried out on the target system may require the installation of additional software, unless the mission can be carried out by functionality provided by the target system's operating system or software that is already installed. If the cyber operation is conducted to take the system down, software installation is usually also not required.

In most cases, the software to be installed on the target system is a *Remote Access Tool* (RAT), which needs to be persistently available in the boot process of the system and which opens a 'backdoor' allowing the intruder to take control. Especially automated attacks install client software on the target system that opens and operates communication channels with, typically, a super-ordinated command and control instance, e.g., the command and control server of a botnet. The installation of such RAT software on a target system faces major challenges since:

- the users and administrators of the target systems should not recognise the RAT tool being installed on their system, so the RAT must be invisible to them;
- the RAT tool must be installed persistently, which means it needs to be able to survive a system re-boot; and
- the RAT tool must be resilient to patches and installations or de-installations of software.

Hiding a RAT is the most important challenge. Once the RAT is detected, the administrators of the target system know that their system has been hacked and they

40 Loaders load software to be executed from a system being controlled by the intruder.

can take actions to remove the RAT. Numerous strategies for hiding RATs have been invented, including:

Installation in system folders replacing known tools:

Installation of RATs in system folders has been a common technique for years. A filename of a well-known[41] operating system tool (e.g., the Windows calculator's 'calc.exe') is used as the filename for the RAT executable, and the original tool is replaced by the RAT. To make this installation even more sophisticated, the original function of the tool might be implemented as well, so if the user manually opens the tool, he will not see a difference in system behaviour. Administrators will find such RATs only if they keep records of original file sizes and installation dates at the time of the operating system installation and compare them in regular intervals against their initial values. Even this information can be manipulated so, to be certain, the only instrument an administrator has is to create databases carrying unique fingerprints of all software installed and to check them on a regular basis.

Installation in temporary folders:

RATs also have been seen in temporary folders. Often, this is the option of choice if full privileges on a system have not been achieved since write permission on temporary folders is often granted or set by default. From there, moving the RAT to a different place on the target system can be considered, once system privileges have been gained. The use of temporary folders on a target system very much depends on the user's behaviour. If a temporary folder is very full and contains a lot of outdated files, it may be a very good place to permanently place a RAT since the users clearly do not clean up their system regularly. However, if the temporary folders are empty or only few files can be found there, a RAT could be easily detected and even deleted by coincidence if the user decides to clean up his temporary files.

Installation in COTS folders:

Modern COTS software consists of multiple files spread through different directories. Users and even administrators rarely know the exact purpose of each file – or which files come with a COTS software at all. This makes it easy for an intruder to hide his payload there, either by replacing an existing file of minor importance or by simply adding a file and giving it a name similar to that of an existing file from the same COTS product to make it appear innocuous. Sophisticated malware will possibly also hide inside COTS software in a way which will not interfere with its original functionality.

Installation in data folders:

A payload can also be hidden in data folders and files. This approach appeared when the IT security industry started to launch products monitoring installation and use of executable files. The user's view of files is usually determined by a filename's suffix;

41 In Windows, the calculator has been used for this for example (calc.exe).

whereas some suffixes indicate executable files (e.g., '.exe'), others indicate specific data formats (e.g., '.docx'). Proprietary data formats without published data format specifications can be misused easily as containers for malware since users and also the majority of administrators will not be able to recognise malicious content. Thus, if a payload is injected into such a file, especially when using older files which have not been used for a long time, it is quite unlikely to be detected.

Once a RAT has been detected, removing it from a stand-alone system is easy and is normally done by a simple re-installation of the machine. Sometimes this is done by restoring it from a backup, which bears the risk of the RAT surviving, if the backup has been made before the RAT was detected but after its successful installation. Since good administrators will also check the backups for traces of the RAT, this is not very likely. Removing a RAT from multiple machines within a network might be more challenging since it is often not possible to shut down the entire network. Trying to restore machine by machine only promises success if the vulnerability the intruder used to exploit the system and install the RAT has been found and can be patched successfully; otherwise, a restored system might simply be re-infected by other machines on the network which have not yet been treated. This gives some indication about the complexity of anti-malware campaigns in larger networks. Considering placement of malicious software in a cloud, backup restoring strategies evidentially are no longer an option. If reinstallation or backup restoring is not an option, the administrators of the target system can try to uninstall the malicious software, or at least patch the system to neutralise the RAT. This might require complex re-engineering of the malware and a test of the patch before going live. Sometimes it is impossible to undo the modifications done by the intruder, especially if more advanced installation methods are used. Notably, RAT functionality is already built-in to some operating systems; Windows, for example, offers remote administration of its systems that can be abused once privileges have been gained.

To strengthen the resilience of a RAT, so-called *rootkits* are used. These are characterised by their capability to hide or remove any traces of their placement, activities and existence. For example, they can modify system logs to not record or to delete all reference to their placement, as well as to disguise all other traces of their existence. A basic way in which rootkits can make themselves difficult to detect is by replacing several standard operating system functions, like files or directory listing functions, with modified versions. For example, a modified version of the 'dir' command,[42] which is used from the command shell to list the files and subdirectories contained in any designated directory, might not display certain files that the intruder wants to keep hidden, or a modified version of the 'procmon' command,[43] which is used to list the current processes on the system, might be designed to not display those processes that are launched by the rootkit. Numerous rootkits have been developed for all common

42 The 'ls' command would be the Linux equivalent.

43 The 'ps' command would be the Linux equivalent.

operating systems. They can be classified into application level, operating system level and BIOS level, and there may be hardware rootkits as well. At present, almost all known rootkits fall into the first two categories; BIOS rootkits are currently being researched intensively, and first prototypes are likely to be seen soon. Such a rootkit would allow access bypassing an operating system, so finding traces there would be impossible. Hardware rootkits are even more difficult to find. These are backdoors implemented in peripheral hardware devices that can be activated remotely without any chance of detection, if details about the command and control functionality of such hardware rootkits have not been made public.

If a rootkit has been placed successfully, and not been detected and removed, the target system is controlled by the intruder and malicious actions of all kind can be conducted. Rootkits and RATs are often combined to maintain access for the intruder persistently. Having installed such a combination on the target system, the intruder can control it and issue any desired command.

2.6 Command and Control – Remotely Control the Target System

If all required software needed for or intended to be used during the cyber operation has been installed on the target system, the planned action needs to be prepared and started. For this, means of command and control have to be foreseen based on which the intruder can submit commands to the target system. They consist of a RAT being installed on the target machine and a control unit being operated by the intruder, together with some means of communication connecting the RAT with the control unit.

Command and control are usually implemented by means of network communication. Since protected systems tend to monitor network traffic and scan it for suspicious activities, command and control are usually hidden in covert channels, where the communication from the intruder to the target machine is embedded in other network communication which appears unsuspicious to firewalls and other IT security products installed on the target system. If rootkits are installed on the target system, communication could also be hidden using this technology, as other sensors set up by the rightful owners of the target systems can record and detect command and control traffic if not covered well enough. Covert channels can be implemented at different abstraction levels. At the network level, command and control information can be embedded into packets of other network communication, for example in packets containing simple requests for a service running on the target system. The installed RAT will intercept this information from the incoming network packets and ‘interpret’ them, i.e. extract the embedded information from the packets. Answers from the RAT will also be encoded into protocol information in response packets sent from the service back to the intruder; this technique is called *tunnelling*. It also works at application level: commands are now hidden in the payload of a network packet. For this purpose, requests are encoded using a secret encoding and decoding scheme that embeds the command

into regular requests for a service, and a response is sent back the same way. The RAT will analyse the content of the requests and extract the embedded command, as well as embed answers in regular service responses. The services used for this purpose will process the intruder's requests as regular requests, not noticing that the only purpose of this communication is the transport of commands for a RAT; therefore, discovery of covert channels is very challenging and needs a lot of experience and sophisticated tools for statistical analysis or tools with a built-in anomaly detection features.

To avoid back-tracing and technical attribution by the target system operators, command and control channels should be established dynamically, and only if needed. Dynamic channels vary permanently, which means that channels are established from different peers each time they need to be used. This can be achieved by the use of multiple command and control units, by changing roles of peers, or by using de-centralised topologies such as peer-to-peer networking with no dedicated servers, and other systems serving as proxies within the communication process. All this can be achieved manually, but botnets are usually used for this purpose.

Apart from network communication, offline command and control can be built into the cyber tool as well. Once delivered and installed, the tool carries all required information to act on the target system. This technique is especially used in logic bombs which are launched against a target and which do not require any link back to the intruder once the cyber tool is engaged. Such cyber tools are also eligible for offline delivery, such as transport through malicious media, or even built into hardware. Offline command and control also plays a role once a covert channel has been discovered and blocked. In this case, specific behaviour can be programmed, such as cyber tool self-destruction (to wipe traces) or system destruction.

2.7 Act – The System is Yours

If intruders can successfully submit commands to the target, the list of possible actions is more or less unlimited. Taking down a system is the most commonly known impact of a cyber attack; the effect is not very challenging for the target system operators since the intrusion is noticed instantly and can usually be countered by restoring the system from a backup or by system re-installation. Still, system downtime and the effort required to bring the system up again can be inconvenient. The same applies for the opposite: information disclosure. Losing business data or even confidential information can harm businesses as well as government entities or private users. As seen with *Operation Red October*, cyber tools can remain undetected for a long time if covert channels are used for the data extraction. Such an effect will often be much more disturbing than a system take down.

The most challenging intrusions are modifications that compromise a system and force operators of the target system to work intensely to figure out which modifications to

data or software have been made, and to distinguish valid data from invalid data. The biggest challenge here is the reverse proportion of acting effort against reacting effort: simple modifications can disorganise target systems entirely and make them useless to their rightful owners. The following examples of disturbing actions which intruders have performed illustrate the great variety of possible actions from which they can choose, once they have successfully exploited the target system:

Renaming files:

Big companies or organisations store their files on servers. A very vicious interference is to rename files or exchange file names of existing documents, either randomly or following a plan. The effect increases if the intruder does not initially do this with files that are currently or recently used but focuses on older files, so the changes are not seen immediately. In that case, the modifications might also be applied to the backup device, so when the attack is finally recognised, restoring the backup does not solve the problem.

Changing file versions and dates:

In any office environment, documents usually have different versions. Substituting this information or swapping new with old versions can entirely disorganise business processes until the cyber attack is detected.

Modifying tables and charts in files:

This effect takes the already introduced effects to a more fine-grain level: all modifications can be done at file level as well. Inserting false data or modifying information in documents can disturb business processes and such changes – if done at system level, so the modifications are not reflected in the file system – are even more difficult to detect.

Deleting single files:

Instead of taking down an entire system, deleting single files can cause more confusion, though the effect is not great if the system is backed up regularly.

Inserting bogus files:

Instead of deleting information, adding some information is also likely to cause confusion, especially if this information is well-prepared and fits into the context of the business processes of the target systems. Such additional information can be, for example, new versions of existing documents or entirely bogus documents introducing new processes or workflows. Malware spreading techniques have been implemented this way, but since that promotes detection, such techniques are no longer used.

Modifying user privileges:

Modifying user privileges is especially effective when granting more right to users than they should have. They tend to misuse their new privileges or accidentally make use of them causing damage to the system. Taking rights from users is not a

very efficient technique since they will complain; system administrators will help out and probably detect the intrusion at the same time.

Changing passwords:

Password changes of target system user accounts, often referred to as famous intruders' activities, are not very effective since they can easily be changed again by the system administrators. The picture changes if all system administrator passwords are changed. In such a case, as with system takedown, only restoring the system from a backup or a system re-installation will help.

Uninstalling software:

Whereas during a cyber operation additional software might have been installed, uninstalling software or applying bogus software patches can have reasonable effects on the target system, especially if system security software is being compromised. Additionally, introducing software failures in COTS software is very efficient if, for example, the undo function is also disabled, and bogus functionality affects information when working with business data.

This list of possible actions and effects is of course incomplete and only demonstrates the potential impact an intruder can have on a target system. The described effects only refer to impacts in cyberspace. If the target system is steering the controls of a machine, for example, the impact may be worse. Successful intrusion into control devices of machines have been seen already, and with the Stuxnet case[44], scenarios of cyber tools indirectly causing physical damage to critical infrastructures are no longer science fiction. Critical infrastructures are of course well protected, and cyber tools designed for such targets require a lot of resources in terms of experts, budget, and test stages, which significantly limits the number of groups or entities capable of performing cyber operations at that level. Nevertheless, in the context of the so-called *Internet of Things*[45], it becomes obvious that computers are now omnipresent and more or less any object with a processor might fall victim to intrusion and manipulation – e.g., a modern car can be deemed a computer on wheels. The good news is that the complexity of cyber tool design in critical areas often only allows attacks against selected single targets only. Also, once a tool has been used and the exploited vulnerability has been detected, the technology used for the cyber operation is known and will be patched, so no further exploitation of the vulnerability is possible, and the cyber tool design using this exploit becomes useless.[46] The picture is different with regard to mass-produced digital products. An attack launched by a botnet against a vulnerability of a product

44 The European Union Agency for Network and Information Security (ENISA) published a Stuxnet Analysis – see internet portal of ENISA. Available: http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis.

45 The concept of the Internet of Things (IoT) has been illustrated, e.g., by CISCO on their internet portal. Available: http://share.cisco.com/internet-of-things.html.

46 This is, among others, the reason why sophisticated exploits remove themselves from the target system after a successful penetration.

which is part of the 'Internet of Things' can compromise millions of systems and cause enormous damage before it is detected, as embedded systems often rely on a specific hardware architecture used in hundreds of different products. An exploit of such a system might expose all products using parts of this architecture to the same cyber tool; for example, a vulnerable digital sensor for temperature connected to a network can be exploited in a car, in a microwave, or in an aircraft. Embedded systems often need to be small and cheap, so neither space nor budget is available for enhanced protection mechanisms. After a successful penetration of the target system, the effects of the intrusion are only limited by the technical capabilities of the targeted system. Whereas security researchers usually do not modify anything on the target since they more or less aim to work out a proof of concept, and State actors will act in accordance with their duties, malicious hackers will try to make a profit.

3. Cyber Operations – A Continuous Improvement Life-Cycle

The stages of a cyber operation might leave the impression that it is a sequential process consisting of consecutive actions; unfortunately, in practice it is not. Multiple iterations within stages and looping back to previous stages are often necessary, for example, to adjust or improve cyber tools. During each stage, new information is gathered which updates the cyber situational picture. This information needs to be evaluated to refine the picture in the best possible manner in order to allow the creation of a precise cyber tool which will be continuously tested on a simulated target built upon the gathered information. An exploit working on the test system, but not in real life, may not only be noticed by the target system operators, but also shows that the information collected is either wrong or insufficient. Sometimes it is not possible to acquire all necessary information. In such cases, missing information can only be substituted by simply guessing or by 'brute-forcing' – a time-consuming practice of trying all possibilities.

At this point, it becomes obvious why hacking is often considered to be more of an art than a science: it is the instinct of a talented hacker that helps him to guess the right path to success. In many cases, a cyber operation will not only target a single dedicated system, but one consisting of multiple machines in a network. Those cases will require much more reconnaissance, and any information found on a single system that has been successfully infiltrated can be used to build cyber tools for other machines within the target network. Especially in the latter case, it is essential to always have a current structured situational picture containing all available information. If information from different sources is being used, quality metrics like age of information or level of trust (e.g., if information is provided by a foreign source) have to be added, as well as verification mechanisms to identify false information which a defence system of the

target may have provided.[47] Again, all these metrics are helpful and necessary, but it is the experience and the feeling that helps to identify and avoid traps.

The continuous improvement does not only cover the tools: techniques are also refined during a cyber operation depending on the findings of scans of the target systems. Since all machines in target networks are likely to be administrated by the same operators, findings concerning one machine can help to improve the techniques used in different stages on other machines since the setup of the system might be the same or similar as the one that has been successfully infiltrated. Similarities are often seen in terms of installed software, running services, file system structure, or even the use of passwords. This all helps to accelerate reconnaissance, and thus to supply suitable cyber tools to conduct the operation swiftly and successfully.

In this chapter, actors as well as methods used for operations in cyberspace were introduced and explained using the *Cyber Kill Chain* model as a blueprint. After pointing out the different roles of cyber actors and the implications their roles have on the conduct of a cyber operation, the stages of such an operation in cyberspace have been described. For each stage, common techniques used by the different actors have been explained and examples of the most commonly used tools have been given. Additionally, the effects caused by these tools and techniques have been discussed, especially the possible actions following a successful target system penetration. This chapter also demonstrated that a cyber operation is a very complex endeavour and requires not only deep system knowledge at expert level, but also a certain portion of talent to be truly successful. Hacking can only be learned up to a certain level; the rest is based on experience and intuition. Therefore, State actors have changed their approach: instead of training their personnel to become cyber actors, they tend to hire cyber specialists from the labour market. This is a challenge since they are competing with businesses and industry, and the few talented candidates available may not necessarily see themselves on a government payroll.

The examples of effects that cyber operations may cause illustrate the threatening technical possibilities an information society is facing. The tools and techniques used to cause these effects are available on the internet and can be used by any talented actor, regardless of the particular intention or motivation. Hacking is not a myth: it happens, and it happens every day. It happens on every continent and in every State, it happens in business and industry, in government entities and on private computers. It happens in factories, pharmacies and embassies. State actors' cyber operations must be accepted as a consequence of the emerging threat to which everyone is exposed, and technical evolution will raise their importance. This chapter has also shown that, due to the design principles of modern computers, it is not possible to find a technical solution

47 A very good introduction into the concept of these 'honeypots' can be found on the SANS internet portal. Available: http://www.sans.org/security-resources/idfaq/honeypot3.php.

to entirely secure an IT system. This applies to both the state-of-the-art platforms and to architectures of the next generation as currently designed. Thus, at present, the only chance to stay competitive – in terms of both active and defensive cyber operations – is to catch up in terms of resources, personnel recruitment and training in methods, techniques and tools to conduct cyber operations as illustrated and explained in this chapter.

Part II

Rights and Obligations of States in Cyberspace

Katharina Ziolkowski

General Principles of International Law as Applicable in Cyberspace

1. Introduction

The present chapter* describes general principles of international law and illustrates their application to cyberspace. For the purposes of the present analysis, cyberspace is understood as a global, non-physical, conceptual space, which includes physical and technical components, i.e., the internet, the 'global public memory' contained on publicly accessible websites, as well as all entities and individuals connected to the internet. Cyberspace has political, economic, social and cultural aspects going far beyond the notion of a pure means of information transfer.

Some claim (inadequately, as the present volume proves) that cyberspace is not or is only partly regulated by law, as cyber-specific international custom is absent and contractual regulation scarce. The classical international law approach to such a situation would be to invoke the basic principle as stated in 1927 by the Permanent Court of International Justice (PCIJ) in the *Lotus*[1] case: based on the notion of sovereignty, in the absence of a legal prohibition, a State enjoys freedom of action. However, the consequently competing freedoms of the coexisting sovereign States are guided (and de-conflicted) by general principles of international law. These principles are most important in the cyber context, since they form the basis for a progressive development of international law, enabling the international law system to respond to the dynamic needs of an international society and especially to meet the fast growing technological advances.

In the following, the nature of general principles of international law will be described (2), followed by an examination of several specific principles and their application to cyberspace, focusing the aspects relevant to international peace and security (3). Thereafter, a few thoughts on *lex ferenda* for cyberspace, in terms of an application of general principles of international law deducted from legal regimes governing shared resources or common spaces, will be presented (4). These sections will be followed by some concluding remarks (5).

* Due to limited research resources, the assessment of secondary legal sources is primarily based on scholarly writings available online. The author is deeply indebted to the NATO ACT - SEE Legal Office for providing access to various online databases.

1 cf *The Case of the S.S. 'Lotus',* Merits (1927) PCIJ Rep Ser A, No 7, 18ff.

2. Nature

The term 'principles' may refer to a meta-legal concept, generated within a philosophical or ethical discourse, or to principles inherent in or developed from a particular body of law or law in general.[2] General principles of international law belong to the latter category, and must be distinguished from the notion of 'justice' (or equity in the broad sense) and from 'general principles of moral law', i.e., compelling or essential ethical principles endorsed in international law (e.g., prohibition of genocide).[3] On a conceptual level, though, the ethical and legal meaning of the term 'principles' cannot be completely separated, as legal principles are always to be deemed as expressions of overarching values.[4] General principles of international law reflect a genuine morality and the most basic values of the international society as inherent in the international order and absolute principles relative to that existing order.[5] It should be mentioned that, because of this feature, general principles of international law are partly criticised in academic writings as being a 'gateway into the legal discourse for natural law maxims'.[6]

As stated by one scholar, 'general principles of law [...] [are] arguably the most important but certainly the least used and most confused source of law [...]'.[7] The jurisprudence of the International Court of Justice (ICJ) does not bring clarity to the matter, as hitherto the Court's reference to general principles of international law has been 'inconsistent and confused'.[8] The academic controversy pertains in particular to whether general principles of international law can be deemed a source of law of a normative character or merely reflecting juridical maxims or legal ideas. In addition, there are disagreements over whether they can present a source of obligations for States, whether they are a source of natural law, and which relation they show with regard to that concept; whether

2 Rüdiger Wolfrum, 'General International Law (Principles, Rules, and Standards)' in idem (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press 2008, online edition [www.mpepil.com]) [in following MPEPIL] MN 6; idem, 'Sources of International Law' in MPEPIL MN 33.

3 Brian D. Lepard, *Customary International Law. A New Theory with Practical Implications* (Cambridge University Press 2010) 165; Mahamoud Cherif Bassiouni, 'A Functional Approach to General Principles of International Law' (1990) 11 Michigan Journal of International Law 768, 775. The ICJ has made a distinction between legal rules and 'moral principles' which can be taken into account 'only in so far as these are given a sufficient expression in legal form', see *South West Africa,* Second Phase (1966) ICJ Rep 5, para 49.

4 Armin von Bogdandy, 'General Principles of International Public Authority: Sketching a Research Field' (2008) 9 German Law Journal 1909, 1912; Bassiouni (n 3) 775.

5 Lepard (n 3) 164; Bassiouni (n 3) 784ff (with further references); Stephen C. Hicks, 'International Order and Article 38(1)(c) of the Statute of the International Court of Justice' (1978) 2 Suffolk Transnational Law Journal (1) 1, 24ff and 27.

6 Niels Petersen, 'Customary Law Without Custom? Rules, Principles, and the Role of State Practice in International Norm Creation' (2008) 23 American University International Law Review 275, 292 (with further references).

7 Hicks (n 5) 7. For reasons of correctness, it should be noted that Hicks refers specifically to '*general principles of law recognized by civilized nations* [pursuant to] Article 38(1)(c) of the Statute of the International Court of Justice', however, the context allows us to conclude that he interprets the norm as including also the notion of general principles of international law.

8 ibid 34.

they are enshrined in Article 38(1)(c) of the *Statute of the International Court of Justice* of 1945 (ICJ Statute), or are part of customary international law within the meaning of Article 38(1)(b) of the ICJ Statute, even of a peremptory character, or whether they exist aside from the enumeration of the aforementioned Article as an autonomous source of law; and whether they have a merely persuasive authority of interpretative guidance or have the a nature of a *quasi*-constitutional norm of the most importance.

Thus, it is surely not an exaggeration to assert that every aspect of general principles of international law is disputed and unclear. Against this background, a thorough presentation of diverse scholarly opinions on the specific aspects of controversy, as well as a clarification with regard to the respective legal debate must be considered a task for a legal analysis of a major extent and cannot be provided for within the limited scope of the present chapter. Therefore, the following assessment can only offer a limited overview of the relevant court rulings and opinions of legal commentators, and attempt to describe the source and content (2.1) as well as the normativity and categorisation (2.2) of general principles of law, the distinctive status they enjoy within the international law system (2.3), and their feature as a vehicle of progressive law development (2.4).

2.1 Source and Content

'[G]eneral principles of law recognized by civilized nations' within the meaning of Article 38(1)(c) of the ICJ Statute are a (subsidiary)[9] source of international law which is derived, according to the wording and as understood by the majority of scholars, from principles common to the domestic law systems of all 'civilised'[10] countries, in so far as they are applicable to inter-State relations.[11] Some scholars assert that the provision (formerly Article 38 No. 3 of the *Statute of the Permanent Court of International Justice*

9 Alain Pellet, 'Art. 38' in Andreas Zimmermann et al (eds), *The Statute of the International Court of Justice. A Commentary* (Oxford University Press 2006) MN 290; contra: Giorgio Gaja, 'General Principles of Law' in MPEPIL (n 2) MN 21.

10 The reference to 'civilised' nations was included in Article 38 of the *Statute of the Permanent Court of Justice* (League of Nations) of 13 December 1920 (and was reproduced in the *Statute of the International Court of Justice*). During these times of Euro-centric international law understanding, it was meant to exclude the rather 'primitive' law systems; nowadays, it does not have any discriminatory meaning, cf Wolff Heintschel von Heinegg, 'Die weiteren Quellen des Völkerrechts' in Knut Ipsen (ed), *Völkerrecht* (6th edn, CH Beck 2010) § 17 MN 2. However, Bassiouni claims that the expression still has utility when a given nation, because of peculiar historical circumstances, no longer follows its previously 'civilised' system of law, or that of the other 'civilised nations'. cf Bassiouni (n 3) 768.

11 James Crawford, *Brownlie's Principles of Public International Law* (8th edn, Oxford University Press 2012) 34ff (with further references on the different opinions); Heintschel von Heinegg (n 10) § 17 MN 1; Pellet (n 9) 251; Robert Kolb, 'Principles as Sources of International Law (With Special Reference to Good Faith)' (2006) 53 Netherlands International Law Review (1) 1, 10; Lepard (n 3) 164; Wolfgang Friedmann, 'The Uses of "General Principles" in the Development of International Law' (1963) 57 American Journal of International Law 279, 282. General principles of law are, eg, responsibility and reparation for damages, unjust enrichment, property and indemnity, cf Heintschel von Heinegg (n 10) § 17 MN 4; other proposals at Friedmann (see above) 287. Additionally, general principles of law contain a multitude of rules of procedural nature, as confirmed by the PCIJ and ICJ in a number of cases, see overview at Gaja (n 9) 8-16.

(PCIJ Statute) of 1920)[12] also includes general principles of international law, reflecting rather the international order of States than the national law systems.[13] They refer to the PCIJ Statute's *travaux préparatoires* of 1920, which show that the drafters had different views of the reference to 'general principles of law', including the notion that the principles are to be understood in a broad way as 'maxims of law'.[14] Furthermore, the drafting history shows that Article 38(c) (or as it was then, No. 3) was a response to the need for the completeness[15] of the law and the intention of the drafters was to avoid a *non liquet* of the Court for lack of a positive rule (however, without giving the judges the possibility to legislate or opening a gateway for natural law).[16] In this spirit, it is asserted that a modern interpretation of Article 38 is justified by the changes of the structure of the legal order since 1920 with regard to the means of determination of international rules based on an implicit consensus of States, which nowadays can be derived from more than the municipal legal systems, e.g., also from binding decisions of international organisations.[17] Finally, it is noted that general principles as mentioned in the ICJ Statute and general principles of international law cannot always be distinguished from each other.[18]

Others[19] assert that the reference to recognition by nations constitutes the distinguishing element between the principles referred to by Article 38(1)(c) of the ICJ Statute and the general principles of international law, of which only the latter derive from international law. Advocates of this approach also invoke the legislative history, object and purpose of Article 38(1)(c) of the ICJ Statute as a supporting argument.[20] Their view is supported by the wording of Article 21(1) of the *Rome Statute of the International Criminal Court*

12 The provision was reproduced in the ICJ Statute without considerable discussion and with only minor alterations (in the numbering of the paragraphs and subparagraphs, instead of alphabetic characters, and the addition of a few words in the introductory phrase). cf Pellet (n 9) 42-45; Gaja (n 9) 4.

13 eg Hicks (n 5) 42; Bassiouni (n 3) 772; Petersen (n 6) 307ff; Wolfrum, 'General International Law' (n 2) 28 (with further references); Crawford (n 11) 37 (asserting that general principles of international law refer to Article 38(1)(c) of the ICJ Statute, as well as to customary law or to certain logical propositions underlying judicial reasoning).

14 On drafting history see Gaja (n 9) 3; Pellet (n 9) 17-41; Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals* (Cambridge University Press 1953) 6-21.

15 In 1920, customary law was considered a slowly developing source of international law. Additionally, the development of new rules of customary law was these days surrounded by scepticism, given the newly appeared heterogeneity of the international community by the establishment of the Marxist-Leninist regime of USSR. Moreover, international treaty law was not as extensive as it is today, as the majority of the treaties (currently over 50,000 are registered at the UN) were concluded after 1945. See Kolb (n 11) 30 (with further references).

16 cf Bassiouni (n 3) 772ff, 779; Petersen (n 6) 307ff; Pellet (n 9) 245 (with further references to the drafting history); Kolb (n 11) 30.

17 Heintschel von Heinegg (n 10) § 16 MN 17, 23; Wolfrum, 'Sources of International Law' (n 2) 10; Pellet (n 9) 96, 88-95 (with further references to ICJ jurisprudence and State practice); Petersen (n 6) 308.

18 Wolfrum, 'General International Law' (n 2) 20; Bassiouni (n 3) 774.

19 eg Pellet (n 9) 86 and 252; Wolfrum, 'General International Law' (n 2) 7 and 20; cf Heintschel von Heinegg (n 10) § 17 MN 1; Hicks (n 5) 3ff, 7, 35; Lepard (n 3) 163 and 166; Gaia (n 9) 32; JP Tammes, 'The Legal System as a Source of International Law' (1953) 1 Netherlands ILR (4) 374.

20 Wolfrum, 'General International Law' (n 2) 28.

of 1998 (Rome Statute), which describes as the law applicable by the Court, *inter alia*, 'principles and rules of international law' (lit. b) and 'general principles of law derived by the court from national laws of legal systems of the world' (lit. c), thus explicitly distinguishing between the two forms of 'general principles'. As the Rome Statute hitherto has been signed by 139 States[21], it can be asserted that the majority of States, who are the primary subjects of international law, consider general principles of international law as existing aside from the general principles derived from national law systems, and consequently beside the enumeration of law sources in Article 38 of the ICJ Statute.

This view is confirmed by the jurisprudence of the PCIJ and ICJ, which indicates the existence of general principles of law, irrespective of their correspondence to principles pertaining to municipal laws.[22] The PCIJ, e.g., referred to 'principles of international law',[23] 'an elementary principle of international law',[24] 'a principle of international law, and even a general conception of law',[25] 'general and essential principles',[26] 'generally accepted principle of international law',[27] and to a 'principle universally accepted'.[28] The ICJ, e.g., invoked 'general and well recognized principles',[29] 'rule[s] of law generally accepted',[30] 'general principles of international law',[31] 'fundamental or cardinal principle

21 Information of the UN Treaty Collection as of 9 May 2013, <http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10&chapter=18&lang=en>.

22 cf Gaia (n 9) 32.

23 Lotus (n 1) 31.

24 *Mavrommatis Palestine Concessions,* Judgement (1924) PCIJ Rep Ser A, No 2, 12 (referring to the principle that a State has a right to protect its subjects when injured by unlawful acts committed by another State).

25 *Case Concerning the Factory at Chorzów,* Merits (1928) PCIJ Rep Ser A, No 17, 29 ('any breach of an engagement involves an obligation to make reparation').

26 ibid 47-48.

27 *Greco-Bulgarian 'Communities',* Advisory Opinion (1930) PCIJ Rep Ser B, No 17, 32 ('in relations between treaty parties treaty law prevails over municipal law').

28 *Electricity Company of Sofia and Bulgaria,* Order (1939) PCIJ Rep Ser A/B, No 79, 199 ('[…] parties to a case must abstain from any measure capable of exercising a prejudicial effect with regard to the execution of the decision to be given, and, in general, not allow any step of any kind to be taken which might aggravate or extend the dispute').

29 *The Corfu Channel Case,* Merits, (1949) ICJ Rep 4, para 22 ('[...] certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war; the principle of the freedom of maritime communications; and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'); *Military and Paramilitary Activities in and against Nicaragua,* Merits (1986) ICJ Rep 14, para 215 ('certain general and well recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war').

30 *Case Concerning Right of Passage over Indian Territory Case,* Preliminary Objections, (1957) ICJ Rep 125, 142 ('Once the Court has been validly seized of a dispute, unilateral action by the respondent State in terminating its Declaration, in whole or in part, cannot divest the Court from its jurisdiction').

31 *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970),* Advisory Opinion (1971) ICJ Rep 16, para 94 ('the general principles of international law regulating termination of a treaty relationship on account of breach').

of [...] law',[32] 'fundamental principle of international law',[33] 'well established principle of international law',[34] and a 'principle universally accepted'.[35] In none of the cases was Article 38(1)(c) of the ICJ Statute mentioned in the context.

The question arises, upon which methodology the existence of general principles of international law is recognised. In the *Lotus* case, the PCIJ conducted 'researches [of] all precedents, teachings and facts to which it had access and which might possibly have revealed the existence of one of the principles of international law […]'.[36] In the *Chorzów Factory* case, the Court ascertained an 'essential principle', because it 'has […] never been disputed in the course of the proceedings in the various cases concerning the Chorzów factory'[37] and 'seem[ed] to be established by international practice and in particular by the decisions of arbitral tribunals'.[38] In the *Electricity Company of Sofia and Bulgaria* case, the PCIJ concluded the existence of a principle, because it was 'universally accepted by international tribunals and likewise laid down in many conventions',[39] without further explanation. The assertion by the ICJ of a general principle of law was only rarely accompanied by an adequate demonstration of its existence in international law.[40] In the *Nicaragua* case, the Court sought a 'confirmation of the validity as customary international law of the principle of the prohibition of the use of force' by reference to Article 2(4) of the *Charter of the United Nations* (UN Charter) and 'the fact that it is frequently referred to in statements by State representatives as being not only a principle of customary international law but also a fundamental or cardinal principle of such law'.[41] In the *Western Sahara*[42] advisory opinion, the ICJ referred as the basis for the principle of international law of self-determination of peoples to the UN Charter, UN General Assembly (UNGA) resolutions and to its own prior decision. Thus,

32 Nicaragua (n 29) 190 ('A further confirmation of the validity as customary international law of the principle of the prohibition of the use of force expressed in Article 2, paragraph 4, of the Charter of the United Nations may be found in the fact that it is frequently referred to in statements by State representatives as being not only a principle of customary international law but also a fundamental or cardinal principle of such law.'); ibid 181 ('common fundamental principle').

33 *Applicability of the Obligation to Arbitrate under Section 21 of the United Nations Headquarters Agreement of 26 June 1947,* Advisory Opinion (1988) ICJ Rep 12, para 57 ('the fundamental principle of international law that international law prevails over domestic law').

34 *Case Concerning Land and Maritime Boundary Between Cameroon and Nigeria Case (Preliminary Objections),* Judgement (1998) ICJ Rep 275, para 38 ('the principle of good faith is a well-established principle of international law').

35 *LaGrand Case,* Judgement, (2001) lCJ Rep 466, para 103.

36 Lotus (n 1) 31.

37 Chorzów Factory (n 25) 29.

38 ibid 47.

39 Electricity Company of Sofia and Bulgaria (n 28) 199 ('[…] parties to a case must abstain from any measure capable of exercising a prejudicial effect in regard to the execution of the decision to be given, and, in general, not allow any step of any kind to be taken which might aggravate or extend the dispute').

40 Gaia (n 9) 20.

41 Nicaragua (n 29) 190.

42 *Western Sahara,* Advisory Opinion (1975) ICJ Rep 12, para 54-65.

it can be concluded that the jurisprudence of the international courts did not develop any methods of identifying general principles of international law. Unfortunately, to quote a scholar, '[s]cholarly writings on this question are few, and what writings exist are unclear.'[43] The most accurate assertion might be the ambiguous proposal to identify general principles of international law 'by way of successive "accretions" (inductive) and "concretization" (deductive) to which the principle leans itself'.[44]

By whichever methodology, academic literature and the jurisprudence of the PCIJ and ICJ indicate that general principles of international law can be derived from general considerations[45] (e.g., 'elementary considerations of humanity', see *Corfu Channel Case*[46]), legal logic (mostly pertaining to procedural rules), legal relations in general (e.g., principle of good faith),[47] from international relations, or from a particular treaty[48] regime (see advisory opinion on *Genocide Convention*[49]).[50] Additionally, some scholars assert that general principles of international law can be derived from the 'conception of [a specific] legal system'[51] (e.g., the UN) and may emerge from 'manifestations of international consensus expressed in [UN] General Assembly and Security Council Resolutions'.[52]

PCIJ and ICJ identified several principles of either general significance (freedom of maritime communications,[53] damages[54]), of a contractual nature (*pacta sunt servanda,*[55] good faith,[56] estoppel[57]), of procedural character (*nemo judex in re sua*)[58] and of

43 Bassiouni (n 3) 817.

44 cf Kolb (n 11) 10.

45 Wolfrum, 'Sources of International Law' (n 2) 37.

46 Corfu Channel (n 29) 22.

47 Wolfrum, 'Sources of International Law' (n 2) 37.

48 ibid (with examples).

49 *Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide,* Advisory Opinion (1951) ICJ Rep 15, 23 ('the principles underlying the Convention are principles which are recognized by civilized nations as binding on States, even without any conventional obligation'); confirmed in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide,* Judgement (2007) ICJ Rep 43, para 161.

50 cf Hermann Mosler, 'General Principles of Law' in Rudolf Bernhardt (ed), *Encyclopedia of Public International Law* (vol 2, Elsevier North Holland 1995) 511-27; Wolfrum, 'General International Law' (n 2) 29; idem, 'Sources of International Law' (n 2) 35.

51 Tammes (n 19) 377ff (referring to the case *Effects of Awards of Compensation made by the United Nations Administrative Tribunal,* Advisory Opinion (1954) ICJ Rep 54).

52 Bassiouni (n 3) 769.

53 Corfu Channel (n 29) 22.

54 Chorzów Factory (n 25) 29.

55 *Article 3, Paragraph 2, of Treaty of Lausanne,* Advisory Opinion (1925) PCIJ Rep Ser B, No 12, 12.

56 *Nuclear Tests (Australia v. France)* (1974) ICJ Rep 253, para 46.

57 *Case Concerning the Temple of Preah Vihear,* Merits (1962) ICJ Rep 6, 31-32.

58 *South-West Africa – Voting Procedure*, Advisory Opinion (1955) ICJ Rep 67, 100 [separate opinion of Judge Lauterpacht].

relevance to specific situations (self-determination of peoples,[59] *uti possidetis juris*,[60] 'fundamental general principles of humanitarian law',[61] 'elementary considerations of humanity'[62]). Academic writings assert, beside the above-mentioned principles, the existence of further general principles of international law, such as consent, reciprocity, unjust enrichment, finality of settlements, and proportionality.[63] Additionally, based on the notion of general principles as systematisation of existing norms of international law, the 'principle of common heritage of mankind' (developed in the context of the law of the sea and applied to certain common spaces) and the 'principle of sustainable development' (developed in the context of international environmental law) are affirmed.[64]

With regard to general principles of international law *as pertaining to international peace and security*, the international courts did explicitly acknowledge the principles of State sovereignty[65] (and the corollary principle of 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'[66]), non-intervention,[67] refraining from use of force in international relations,[68] and peaceful settlement of disputes.[69] Article 2 of the UN Charter enshrines these principles as legal obligations,[70] i.e., the sovereign equality of States (No. 1), non-intervention in matters within the domestic jurisdiction of States (No. 7, although only stating a respective prohibition for the UN), refraining from (threat or) use of force in international relations (No. 4), and peaceful settlement of disputes (No. 3). Article 1 of the UN Charter, depicting the purposes of the organisation, refers to the organisation's goal of achieving international cooperation in solving international problems (No. 3). All the above-mentioned principles of the UN and, additionally, the duty of States to cooperate are

59 Western Sahara (n 42) 54-65; Namibia (n 31) 31 ('[..] the subsequent development of international law with regard to non-self-governing territories, as enshrined in the Charter of the United Nations, made the principle of self-determination applicable to all of them').

60 *Case Concerning the Frontier Dispute,* Judgement (1986) ICJ Rep 554, para 20.

61 Nicaragua (n 29) 218, 220, 225.

62 Corfu Channel (n 29) 22.

63 cf Crawford (n 11) 37; Kolb (n 11) 25ff; Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press 1963) 19. As stated before, it is noted in the academic writings that some of the principles may not be distinguishable from the 'general principles of law recognized by civilized nations' in the meaning of Article 38(1)(c) of the ICJ Statute.

64 Wolfrum, 'General International Law' (n 2) 8.

65 Nicaragua (n 29) 263.

66 Corfu Channel (n 29) 22.

67 Nicaragua (n 29) 202, 204.

68 ibid 181.

69 ibid 290.

70 Andreas Paulus, 'Article 2' in Bruno Simma et al (ed), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012) MN 8.

further elaborated upon in the UNGA *Friendly Relations Declaration*[71] of 1970 (widely accepted as a *quasi*-binding interpretation of the UN Charter),[72] which declares them to 'constitute basic principles of international law' (General Part, para. 3). These 'basic principles' were confirmed by the UNGA in its *Millennium Declaration*[73] of 2000. At the regional level, States participating in the *Conference on Security and Cooperation in Europe* in 1975 adopted a *Declaration on Principles Guiding Relations between Participating States*[74] (part of the so-called *Helsinki Declaration*), which affirms, apart from other principles, all the general principles of international law pertaining to international peace and security as stated in the *Friendly Relations Declaration*. Scholarly writings in general confirm these principles as having the nature of general principles of international law, partly adding also into this category the principle of domestic jurisdiction (corollary of State sovereignty).[75]

Thus, a common core of general principles of international law, as pertaining to international peace and security, can be identified, even if the finding is '[…] based on nothing grander than their having passed what Thomas Franck calls the 'but of course test' – a more or less unstable 'common sense of the international community' […]'.[76] In summary, general principles of international law as relevant to international peace and security can be deemed as consisting of the principles of:

- sovereign equality of States, including the corollary principles of:
  - self-preservation,
  - independence,
  - jurisdiction over domestic matters,
  - non-intervention in matters within the domestic jurisdiction of other States,
  - duty not to harm the rights of other States,

71 *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations* UNGA Res 2625 (XXV) (24 October 1970) annex (adopted without vote).

72 Bardo Fassbender, 'Article 2(1)' in Simma (n 70) MN 31 (referring to the 'careful preparation and adoption by consensus', due to which the declaration 'can be relied upon almost like a text enjoying binding force'). See also Paulus (n 70) 5; Helen Keller, 'Friendly Relations Declaration (1970)' in MPEPIL (n 2) MN 1 (referring to 'codification and progressive development of international law') and MN 31ff (showing the continuous reference to the resolution by UNGA, UNSC, ICJ, etc, with further references).

73 *United Nations Millennium Declaration* UNGA Res 55/2 (8 September 2000) para 4.

74 *The Final Act of the Conference on Security and Cooperation in Europe* (1 August 1975) (Helsinki Declaration) (1978) 14 ILM 1292.

75 cf Crawford (n 11) 37 (naming the principles of equality of States and domestic jurisdiction); Kolb (n 11) 25ff (naming the principles of 'non-use of force, peaceful settlement of disputes […], etc.'); Heintschel von Heinegg (n 10) § 16 MN 43 (naming the principle of equality and independence of States); Brownlie (n 63) 19.

76 International Law Commission (ILC), *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law* (Report of the Study Group of the International Law Commission, finalized by Martti Koskenniemi, UN Doc No A/CN.4/L.682, 13 April 2006) para 468 (with further references).

- maintenance of international peace and security, including the principles of:
  - refrain from (threat or) use of force in international relations,
  - duty to peaceful settlement of disputes, and
- duty to international cooperation in solving international problems.

The significance and concretisation of these principles for cyberspace will be introduced in detail *infra* (section 3).

2.2 Normativity and Categorisation

Some scholars assert that, because of their generality, not all general principles of international law could have a binding authority in the meaning of normative requirements on States, but rather a persuasive authority in the meaning of guidelines.[77] Others, also addressing the general character of the principles, concur with this finding, referring to general principles as mere 'legal ideas'.[78] General principles of international law certainly do not show the level of specification of rules, which are formulated for practical purposes.[79] However, they are also distinct from abstractly formulated legal standards (e.g., 'due regard' or 'reasonable time'). Those legal standards, being 'concepts of law' mostly incorporated in legal norms, do not present a source of law, but support the subsuming of the facts of a case to a norm.[80] In contrast, general principles of international law show a core legal meaning developed over centuries, and thus present neither 'legal ideas' nor mere structural or guiding principles.[81]

However, during the 1960s, it was claimed that general principles of international law could not be deemed a source of law, because the legal principles governing the Western system, the system based on Marxism-Leninism, and the Islamic law system (preconditioned by compatibility with various interpretations of Islam) were very different.[82] In a more general manner, referring to the value-oriented nature of the principles, it was also asserted that a general consensus on values cannot be identified between the members of the international society.[83] Indeed, general principles of international law are characterised by serving the purpose of protecting a common or individual good, and are value-related.[84] However, this cannot be taken as an argument against the normative nature of general principles of international law, as it is true for

77 cf Lepard (n 3) 167.

78 Kolb (n 11) 9.

79 Wolfrum, 'General International Law' (n 2) 6; Kolb (n 11) 9; Cheng (n 14) 24.

80 Kolb (n 11) 16ff, stating that, however, some legal standards as 'equity', 'goodwill' or 'good faith' proved to have been applied autonomously in arbitration of commercial law cases.

81 cf von Bogdandy (n 4) 1912; Kolb (n 11) 8ff.

82 Bassiouni (n 3) 782ff (with further references).

83 Hicks (n 5) 6; Ingo Venzke and Jochen von Bernstorff, 'Ethos, Ethics, and Morality in International Relations' in MPEPIL (n 2) MN 3 and 28.

84 Petersen (n 6) 288.

the whole international law system. According to a broad group of scholars, (basic) universally shared values lay the foundation of international law, aiming at safeguarding and promoting universal values and global goals.[85] Irrespective of the dichotomy of positivism *versus* naturalism, it is acknowledged today that any legal argument has constant recourse to extra-positive elements, which flow into the law by way of 'certain strong arguments or *topoi*, concentrated into a series of value-oriented general principles [...]'.[86] The concerns referring to ideological, religious and other value-based differences within the international society can be contested with a reference to the universal acceptance of the international law system's existence. General principles of international law are inherent to that system (and their general and basic nature allows different interpretations in concrete situations). Nevertheless, it will indeed always be important to delimit them from the extra-positive social or ethical principles,[87] or from the aforementioned 'general principles of moral law'.

All in all, general principles of international law are nowadays accepted by a vast majority of scholars as a normative source of law.[88] This finding is confirmed by the wording of the above-mentioned Article 21(1)(b) of the Rome Statute (declaring 'principles and rules of international law' as a source of law applicable by the International Criminal Court) as well as by the jurisprudence of the PCIJ and ICJ which relied upon general principles of law not only for interpretative purposes, but also to fill a gap in a situation which was not governed by contractual or customary law.[89]

However, controversy prevails with regard to the categorisation of general principles of international law within the sources of law. Some[90] scholars deem general principles of international law as being part of international customary law, even presenting peremptory norms (*ius cogens*) of international custom.[91] Others[92] recognise the principles as a separate source of international law, giving an impulse and directing the formulation of customary international law, however, being most difficult to distinguish from it. The jurisprudence of the ICJ does not support the drawing of a definite conclusion: the Court referred in the so-called *Hostages*[93] case to a principle of

85 Venzke and von Bernstorff (n 83) 28.

86 Kolb (n 11) 4.

87 ibid.

88 ibid; Heintschel von Heinegg (n 10) § 16 MN 43; Hicks (n 5) 11; Petersen (n 6) 277 and 287 (implicitly); von Bogdandy (n 4) 1912; Cheng (n 14) 23.

89 See examples of the jurisprudence at Bassiouni (n 3) 798 (with further references).

90 Heintschel von Heinegg (n 10) §16 MN 43; Tullio Treves, 'Customary International Law' in MPEPIL (n 2) MN 1 and 19-22; Gaja (n 9) 24.

91 Bassiouni (n 3) 780; Crawford (n 11) 37, similar also before Brownlie (n 63) 19.

92 Hicks (n 5) 7, 41; Lepard (n 3) 166; Cheng (n 14) 23.

93 *United States Diplomatic and Consular Staff in Tehran,* Judgment (1980) ICJ Rep 3, para 86 (inviolability of diplomatic personnel and the mission).

international law as being also a norm of customary law. In the *Nicaragua*[94] case, the Court stated that certain customary international law 'flow[s] from a […] fundamental principle'. Then, in the *Nicaragua*[95] case and in the *Frontier Dispute*[96] case, the ICJ referred to 'principles of customary law', *quasi* combining the general principles of international law and international customary law. Finally, the Court also referred to 'general or customary international law' in the *North Sea Continental Shelf*[97] case and ambiguously to 'general international law' in the *Barcelona Traction*[98] and *Hostages*[99] case, thus not making any difference between general principles of international law and international customary law. All in all, it might be wise to concur with those who claim that any intent of a rigid categorisation of general principles of international law would be inappropriate.[100] Depending on the content and use of a principle, it can be part of customary law or a separate and substantive source in itself.[101]

General principles of international law can also present legal rights and obligations.[102] Whereas in national law a distinction is made between a law source as objective law on the one hand and a right, an obligation or a subjective entitlement on the other hand, the two aspects merge in international law due to the lack of a centralised legislator.[103] In the international law system, the community of its subjects, i.e., primarily States, create the legal bonds and are subject to them at the same time.[104] Additionally, general principles as endorsed in Article 2 of the UN Charter directly entail legal rights and obligations on the basis of the binding character of contractual law.[105] However, it could be argued that a general principle of international law will achieve the quality of a right or obligation only after a specific interpretation of its general content in a concrete situation, making it thereby 'operational' in the legal sense.[106] Consequently, general principles of international law as pertaining to international peace and security would unfold their nature as a State's 'hard law' right or obligation in the cyber realm only

94 Nicaragua (n 29) 181, 188, 190 (refrain from use of force in international relations).

95 ibid 290.

96 Frontier Dispute (n 60) 21.

97 *North Sea Continental Shelf,* Judgement (1969) ICJ Rep 3, para 37.

98 *Case Concerning the Barcelona Traction, Light and Power Company, Limited,* Judgment (1970) ICJ Rep 3, para 34, 87 ('body of general international law' 'guaranteed by general international law, in the absence of a treaty applicable to the particular case').

99 Hostages Case (n 93) 62 ('obligations under general international law').

100 Crawford (n 11) 37; Hicks (n 5) 11.

101 Hicks (n 5) 11; Tammes (n 19) 374.

102 Kolb (n 11) 11; Wolfrum, 'Sources of International Law' (n 2) 34 (stating that international and regional courts and tribunals make use of principles as an interpretative tool or as a source of concrete obligations).

103 Kolb (n 11) 11.

104 ibid.

105 Wolfrum, 'General International Law' (n 2) 7; Pierre d'Argent and Nadine Susani, 'United Nations, Purposes and Principles' in MPEPIL (n 2) MN 20.

106 Similarly d'Argent and Susani (n 105) 20 (with regard to principles enshrined in Article 2 of the UN Charter).

after a respective interpretation and thus concretisation of the principle with regard to governmental cyber activities.

2.3 Distinctive Status within the International Law System

General principles of international law are attributed a distinctive status within the international law system, which is, however, based on different approaches to legal reasoning and to international law.

2.3.1 Relationship to Practice, *opinio iuris* and Consent of States

It is widely recognised within scholarly writings that the development or recognition of general principles of international law either does not require proof of their existence, or exists independently from the consent or will of the States.

Based on the consensual approach to international law (i.e., emphasising the importance of the will of the States, who are the primary subjects creating international law), and on the presumption of general principles of international law being part of international custom, some scholars assert that the existence of the general principles is based on the States' *opinio iuris*, which, however, does not require to be evidenced.[107] They affirm that there would be an agreement within the international community that the general principles of international law have been so long and generally accepted and are still believed to be desirable, so there would be no need for an evidence of State practice for their recognition.[108] This approach corresponds with the classical theory of international custom, which perceives State practice not as a normative requirement, but as a means to proving the existence of consent (in the meaning of a tacit treaty).[109] In the case of general principles of international law, such a (tacit) consent or will of the States is presumed.[110]

However, such presumed (tacit) consent or will of the States could also be deemed irrelevant. The above-presented view is based on the notion that the existence of general principles of international law is based on the *opinio iuris* of the States. It is noted within scholarly writings that *opinio iuris* is an opinion, conviction, or belief referring to the legality or illegality of a certain behaviour of a State, thus not depending on the will of the State.[111] It is rather based on a meta-legal notion or on general legal considerations that a certain State's conduct is just, fair or reasonable and, for that reason, required

107 eg Heintschel von Heinegg (n 10) § 16 MN 43; Crawford (n 11) 37; Petersen (n 6) 277 and 285; Wolfrum, 'Sources of International Law' (n 2) 35; Hicks (n 5) 7-11; Lepard (n 3) 166; Brownlie (n 63) 19.

108 cf Heintschel von Heinegg (n 10) § 16 MN 43; Crawford (n 11) 37; Lepard (n 3) 166; Brownlie (n 63) 19.

109 Petersen (n 6) 294ff, 300.

110 Martti Koskenniemi, 'The Politics of International Law' (1990) 1 European Journal of International Law (4) 4, 20-27 (claiming the binding character of general principles of international law and other non-consensual general law because of a 'subjective value of "justice"').

111 Treves (n 90) 9.

under law.[112] Thus, *opinio iuris* is based on a value judgement.[113] General principles of international law, reflecting a genuine morality and most basic values of the international society as inherent to the international order (section 2), would consequently not depend on the (tacit) consent or will (evidenced by State practice) for the proof of their existence.

Furthermore, it is asserted that general principles of international law exist independently of the practice, consent or will of the States, because they form the 'backbone' of the international law system.[114] As the international law system is an accepted reality of the international structure and order, and gives the States the platform to exercise their will, its very existence does not need consent or expression of will by the States.[115] This finding is confirmed by the ICJ, which held in the *Gulf of Maine* case:

> [...] customary international law [...] in fact comprises a *limited set of norms for ensuring the co-existence and vital co-operation* of the members of the international community, together with a set of customary rules whose presence in the opinio juris of States can be tested by induction based on the analysis of a sufficiently extensive and convincing practice, and not by deduction from *preconceived ideas*.[116]

The Court thus distinguished within the customary law a category of 'a limited set of norms for ensuring the co-existence and vital co-operation' of States deducted from 'preconceived ideas', and not from practice, *opinio iuris*, consent or any other expression of the will of States.

Thus, the binding nature of general principles of international law is based either on the assumption of a tacit consent or will of the subjects of international law, i.e., primarily States, or on the notion that the general principles reflect universally accepted meta-legal principles (justice, equity and fairness).[117] This statement reflects the dichotomy of the consensual approach (recognising that international customary and contractual law is firmly based on the States' consent) and a rather natural law approach to international law. This legal dichotomy, which, at first sight, appears to be of academic value only, is especially important in the context of general principles of international law, as some of them, according to jurisprudence of the ICJ and scholarly opinion, are derived from 'preconceived ideas' and apply regardless of the States' practice, *opinio iuris*, consent or any other expression of will.

---

112 Wolfrum, 'Sources of International Law' (n 2) 25; similar Koskenniemi (n 110).

113 Wolfrum, 'Sources of International Law' (n 2) 25.

114 ibid; Treves (n 90) 9; Hicks (n 5) 9.

115 cf Hicks (n 5) 9.

116 *Case Concerning Delimitation of the Maritime Boundary in the Gulf of Maine Area,* Judgment (1984) ICJ Rep 246, para 111 [emphasis added].

117 Wolfrum, 'Sources of International Law' (n 2) 3.

This results in a most significant consequence: States cannot 'opt-out' from general principles of law that are necessary for the 'co-existence and vital co-operation' within the international community. It can be asserted that such principles are reflected by the general principles of international law as pertaining to international peace and security as identified above (section 2.1). After a respective interpretation and concretisation with regard to the cyber realm, as will be provided *infra*, they ought to be observed by States regardless of their (other) practice, *opinio iuris*, consent or any other expression of will.

2.3.2 Higher 'Normative Value'

General principles of international law were described by scholars as 'so fundamental [...] that no reasonable form of co-existence is possible without their being generally recognized as valid', as 'manifestations of the universal legal conscience', or as 'principles that constitute unformulated reservoir of basic legal concepts [...], which form the irreducible essence of all legal systems'.[118] Not surprisingly, advocates of the constitutionalist approach to international law attribute general principles that are essential for the existence of the present order structure a *quasi*-constitutional role within the international law system.[119] Such principles would be, e.g., good faith, proportionality, restitution of unjust enrichment, self-determination of peoples, non-use of force, and peaceful settlement of disputes.[120] The constitutionalist approach distinguishes such 'constitutional norms' from other norms of international law and pronounces a priority of values which shall reflect a hierarchy of norms.[121] The respective debates are characterised by controversy that can be related to diverging underlying conceptions of the relationship between morality and international law.[122]

Independently from the constitutionalist approach, some authors also claim that certain fundamental principles of international law would in theory present a superior source of law.[123] This view is based on the notion that such basic principles would be applied for the purpose of modifying and superseding conventional and customary rules, as the principles would, due to their general character and value-based content, present the standard for testing the conformity of other norms with the existing legal basis.[124] For

118 Bassiouni (n 3) 771 (with further references).

119 Kolb (n 11) 9, 25 and 36 ('The law of general principles is constitutional law in the fullest sense of the word. It is placed on the level of sources, of development of the law, of essential metabolistic functions within the legal order.').

120 ibid 25ff.

121 Venzke and von Bernstorff (n 83) 17.

122 ibid.

123 Martti Koskenniemi, 'Hierarchy in International Law: A Sketch' (1997) 8 European Journal of International Law 566, 577; Wolfrum, 'Sources of International Law' (n 2) 11; Bassiouni (n 3) 787; Hicks (n 5) 29; Cheng (n 14) 22.

124 Hicks (n 5) 29; Bassiouni (n 3) 787.

the same reasons, they could not be overridden by any other individual rule, however specific and enacted in formal fashion.[125]

A formal hierarchy between the sources of international law must be rejected.[126] The informal hierarchy in the techniques of legal reasoning (i.e., successive orders of consideration based on ease of proof or on the approach to applicable law, proceeding from more specific to more general norms) does not introduce a hierarchy of norms.[127] Also the UN Charter, enshrining some of general principles of international law (section 2.1), cannot be viewed as a constitution or basic norm of international society at a higher normative level. The Charter is an international treaty, which – according to its Article 103 – prevails only over contrasting contractual obligations taken by a UN Member State.

Furthermore, it is asserted that a 'heightened normativity' of certain general principles of international law could be derived from their character as peremptory norms (*ius cogens*) of international customary law.[128] The notion of *ius cogens* was first proposed by (natural law) scholars in the 17th and 18th century and was adopted in the *Vienna Convention on the Law of Treaties* (VCLT) of 1969.[129] According to Article 53 of the VCLT, *ius cogens* is '[...] a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character.' Given that norms, which are 'accepted and recognized by the international community of States as a whole' are based on the consent, or at least acquiescence, of the world, the *ius cogens* concept is based on the consensual foundation and not on the notion of a gateway of meta-legal or general considerations (as envisioned by the naturalists).[130] Though, *ius cogens* also indicates a certain recognition of a 'public order of the international community' based on the consensus concerning fundamental values which are not at the disposal of the subjects of that legal order.[131] Despite this distinctive nature, and in contrast to some assertions within scholarly writings,[132] *ius cogens* is not a higher category of formal sources of international law, but a particular quality of customary law norms.[133] This particular quality is not depicted by a hierarchical position, but by special consequences of the breach of the norms, as stated in Article 53 of the VCLT with regard to contracts and in Articles 40 and 41 of the *Draft Articles on*

125 Koskenniemi (n 123) 577.

126 Pellet (n 9) 265 and 268; ILC (n 76) 463 (and 85 for more detailed information); Cheng (n 14) 22ff.

127 Koskenniemi (n 123) 566-582; ILC (n 76) 463.

128 Crawford (n 11) 37; Bassiouni (n 3) 780; Brownlie (n 63) 19.

129 Wolfrum, 'Sources of International Law' (n 2) 49; Jochen A Frowein, 'Ius Cogens' in MPEPIL (n 2) MN 3; ILC (n 76) 361.

130 Wolfrum, 'Sources of International Law' (n 2) 49.

131 Frowein (n 129) 3, 11.

132 Wolfrum, 'Sources of International Law' (n 2) 11; Cheng (n 14) 22.

133 Pellet (n 9) 279.

Responsibility of States for Internationally Wrongful Acts[134] of the International Law Commission (ILC) with regard to 'serious breach[es] by a State of an obligation arising under a peremptory norm of general international law'. Thus, it can be concluded, that, although there is no hierarchy among the sources of law, there is a notion that *ius cogens*, because of its fundamental content, is in one way or another intrinsically 'superior' to all other norms.[135]

Scholars are in disagreement as to what constitutes *ius cogens* and how a given rule, norm or principle rises to that level.[136] Significant State practice, which could support the identification of specific peremptory norms, has not developed.[137] Nonetheless, it is asserted that fundamental general principles of international law have the character of *ius cogens* (and are even 'merely a semantic variation'[138] of them).[139] This is based on the understanding of fundamental principles of international law as norms 'whose perceived importance, based on certain values and interests, rises to a level which is acknowledged to be superior, and thus capable of overriding another norm, rule, or principle in a given instance'.[140] This view could be deemed as confirmed by the ICJ, which stated in the *Nicaragua*[141] case 'that […] the customary international law flow[s] from a […] fundamental principle outlawing the use of force in international relations', i.e., a prohibition which is widely acknowledged as a *ius cogens* norm.

Thus, fundamental principles of international law can be attributed a 'higher normative value' – without introducing a formal hierarchy into the sources of international law – either because of their *quasi*-constitutional role within the international law system, or as peremptory norms of international custom. Taking either approach, there seems to be an understanding within the academia and within the rulings of international courts that the fundamental principles of international law do have a non-derogative character. This, as mentioned above, results in the finding that all States' behaviour has to be guided by the general principles of international law, and, whenever they also show a normative character in terms of a legal obligation, States cannot 'opt-out' from fundamental principles of international law, i.e., those which are essential for the

134 UNGA Res 56/83 (12 December 2001) annex.

135 Pellet (n 9) 280.

136 Bassiouni (n 3) 801ff (with further references). In its Commentary to the *Draft Articles on State Responsibility* of 2001, the ILC gave as examples of peremptory norms the prohibition of aggression, of slavery and slave trade, of genocide, racial discrimination and apartheid, of torture, as well as basic rules of international humanitarian law applicable in armed conflict, and the right to self-determination, see ILC, *Draft Articles on State Responsibility* UN Doc 56/10, commentary on Article 40, para 4-6. In scholarly writings also the right to self-defence and the prohibition of piracy are frequently qualified as *ius cogens,* cf ILC (n 76) 374 (with a multitude of further references in footnote 522).

137 Wolfrum, 'Sources of International Law' (n 2) 50.

138 Bassiouni (n 3) 780.

139 ibid; Crawford (n 11) 37; Brownlie (n 63) 19.

140 Bassiouni (n 3) 805.

141 Nicaragua (n 29) 181, 188, 190 (refrain from the use of force in international relations).

'co-existence and vital co-operation of the members of the international community'. This finding is of significance for the principles as pertaining to international peace and security in cyberspace, as they will show a 'normative value' higher than other obligations deriving from international law.

2.3.3 Relationship to the Concept of Fundamental Rights and Duties of States

A different theoretical approach to the phenomenon of a 'higher normative value' of the fundamental principles of international law is given by the concept of fundamental rights and duties of States.

The doctrine emerged in the 17th century (coinciding with the Peace of Westphalia of 1648, marking the beginning of modern international law) and is based on the independence (from papacy and empire) and equal sovereignty of States (with regard to their exclusive dominion of territorial jurisdiction).[142] According to the concept, the existence of fundamental rights and duties is inherent to the essence of a State.[143] The specification of the nature of such fundamental rights and duties is problematic, as pursuant to the doctrine, they would present a *quasi*-constitutional basis, upon which all other international law norms are based.[144]

At the beginning of the 20th century (and especially on the American continents) several inter-governmental conferences dealing with fundamental rights and duties of States were conducted, resulting in respective political declarations.[145] Additionally, diverse international lawyers' associations developed declarations of fundamental rights and duties of States.[146] Also, several international treaties codifying States' views on fundamental rights and duties were concluded.[147] In 1949, the ILC elaborated

142 Sergio M Carbone and Lorenzo Schiano de Pepe, 'States, Fundamental Rights and Duties' in MPEPIL (n 2) MN 3; ILC (n 76) 1-4.

143 Carbone and Schiano de Pepe (n 142) 1 and 30; Volker Epping and Christian Gloria, 'Der Staat im Völkerrecht' in Ipsen (n 10) § 26 MN 1.

144 Epping and Gloria (n 143) § 26 MN 2.

145 eg *Declaration of American Principles of the Eights International Conference of American States* of 1938. For more information see ILC (n 76) 149-153.

146 eg American Institute of International Law in 1916 (*Declaration of Rights and Duties of Nations*); the International Juridical Union in 1919 (*Draft of a Declaration of Rights and Duties of Nations*); the International Commission of American Jurists in 1927 (Report *Project II, States: Existence, Equality, Recognition*); the Union Juridique International/International Law Association in 1936, or the Inter-American Juridical Committee in 1942 (*Reaffirmation of Fundamental Principles of International Law*). For more information see Carbone and Schiano de Pepe (n 142) 6; ILC (n 76) 156ff.

147 eg the *(Montevideo) Convention on Rights and Duties of States* (inter-American) of 26 December 1933; the *Charter of the Organization of American States* of 30 April 1948 (Chapter IV), or the *Charter of the Organization of African Unity* of 25 May 1963 (Article III and V; abrogated in 2000 by the *Constitutive Act of the African Union*). Article III of the OAU Charter (*Principles*) referred to sovereign equality, non-interference, peaceful settlement of disputes; Article V (*Rights and Duties of Member States*) referred to equal 'rights and duties of Member States'.

(upon request of the UNGA)[148] a draft *Declaration on the Rights and Duties of States*[149] containing 14 articles, which was transmitted by the UNGA to States for considerations on further action. However, already within the ILC the draft was voted against (only) by the US and the USSR, and States never requested the UNGA to take the issue up again.[150] It should be mentioned that, according to the draft's preparatory work, the ILC considered Article 2 of the UN Charter as expressing fundamental rights and duties of States.[151] In the same line, the *Friendly Relations Declaration* could be seen at first sight as reflecting fundamental rights and duties of States.[152] However, despite mentioning 'rights and duties of Member States under the [UN] Charter' (General Part, para. 2) the declaration is drafted in terms of 'basic principles' rather than of 'rights and duties' (section 2.1).

Summarising the different treaties, declarations and drafts, the catalogue of the fundamental rights and duties of States can be deemed to comprise:[153]

- equal sovereignty,
- independence,
- jurisdiction,
- non-intervention,
- refrain from (threat or) use of force,
- self-defence (also in the broader term of self-preservation),[154]
- peaceful settlement of disputes,
- mutual respect of the rights of all,
- immunity of ambassadors,
- *pacta sunt servanda*,
- good faith,
- (respect for human rights and fundamental freedoms).[155]

Scholars have asserted the fundamental rights and duties of States as forming part of general principles of international law that aim at governing the friendly and peaceful coexistence and cooperation of States, and have described them as being objective, independent of any expression of willingness by States, particularly inalienable and

148 UNGA Res 178 (II) (21 November 1947) para 3.

149 UNGA Res 375 (IV) (6 December 1949) annex.

150 Carbone and Schiano de Pepe (n 142) 14; Fassbender (n 72) 30.

151 ILC (n 76) 140.

152 Epping and Gloria (n 143) § 26 MN 5.

153 The assessment is based on the texts of the aforementioned treaties and declarations, especially the draft declaration prepared by the ILC for UNGA (n 149) as well as on scholarly writings.

154 Carbone and Schiano de Pepe (n 142) 28.

155 eg Article 6 of the ILC draft declaration (n 149).

absolute in nature.[156] Indeed, content-wise and with regard to the distinctive status claimed for the fundamental rights and duties, they resemble the general principles of international law that are essential for the 'co-existence and vital co-operation of the members of the international community'.

The relevance of the doctrine of fundamental rights and duties of States can be judged as minimised by the emergence of international law subjects other than States (i.e., international organisations), by the increasingly complex (contractual) interaction and interdependence of States in times of globalisation impairing their sovereignty, and perhaps also because of its natural law ascendancy. However, the contents, i.e., the legal independence and equal sovereignty as well as the principles deriving from this basic foundation, remain crucial to the functioning of the international order.

Thus, despite the different doctrinal approach, the concept recognises the notion that some basic principles form the very foundation of the international law order. Content-wise the fundamental rights and duties of States resemble the principles identified within the scholarly writings as 'constitutional', of 'higher normativity', and those essential for the 'co-existence and vital co-operation of the members of the international community' (section 2.3.2).

2.4 Instrument of Progressive Law Development

General principles of international law may serve different purposes. They are a normative source of law, which governs situations not regulated by formulated norms.[157] By introducing overarching considerations into international law, they also serve as a guideline or framework for interpretation of conventional and customary international law.[158] For the same reason, they have the function of systematisation of law, in the meaning of amelioration of the fragmentation of international law.[159] However, the most important feature of general principles of international law is their function as a basis for the progressive development of international law.[160] This feature is especially significant in the realm of international peace and security in the cyber context, as cyber specific customary law is absent and contractual regulation scarce.

General principles of international law have the necessary degree of abstraction and concreteness to be able to be dynamic yet filled with a certain legal meaning.[161] Their generality and flexibility enables the principles to be the means of substantial,

156 Carbone and Schiano de Pepe (n 142) 30ff; Epping and Gloria (n 143) § 26 MN 3.

157 Wolfrum, 'Sources of International Law' (n 2) 34ff; idem, 'General International Law' (n 2) 20; Bassiouni (n 3) 775ff; Cheng (n 14) 390.

158 ibid.

159 Wolfrum, 'General International Law' (n 2) 7 and 20.

160 ibid.

161 Kolb (n 11) 9.

progressive development of international law.[162] Such development can occur by progressive interpretation of international law guided by the principles, as there is (apart from relatively few exceptions) no law-application without some law-creation.[163] General principles of law may also be the starting point for the evolution of a new rule of customary law and thus play the middle role between *lex lata* and *lex ferenda*.[164] Last but not least, general principles can also serve *per se* as a basis for the development of new rights and obligations.[165] Especially in the absence of relevant international practice and of applicable specific rules, the recourse to general principles of international law is the only option for not leaving a specific situation in a legal *lacuna*. Considering the inherent limitations for the modifications of treaty law as well as of customary international law, general principles of international law can be thus deemed as 'transformators' of rising extra-positive (social, moral, etc.) needs of the international community into international law by subsuming the new situation to a principle and by a deduction or reception from the principle.[166] This way, general principles of law play a prominent role in legal dynamics, in the development of the law, in the adaptation of law to new situations, and consequently in the filling of the *lacunae*.[167] They prevent a static application of archaic norms in a legal system which needs to respond to the dynamic needs of the international society, especially to meet the needs of fast growing technological advances.[168]

The development of international law by a modern interpretation of the general principles (or creation of new sub-principles) will not occur in the abstract, but as a reaction to practical needs and specific phenomena that calls for development. The 'emergence' of cyberspace and its relevance for international peace and security justifies a re-consideration of that particular body of law. Thus, the new phenomenon of cyberspace as a new common space for inter-State relations, results in the need of a fundamental regulation as pertaining to the international peace and security. In this regard, a modern interpretation of the respective general principles of international law will support the progressive development of international law.

3. Specific General Principles of International Law as Applicable in Cyberspace

In the following, the aforementioned general principles of international law as pertaining to international peace and security (see section 2.1), namely sovereign equality of States

162 ibid; Wolfrum, 'Sources of International Law' (n 2) 39; Bassiouni (n 3) 804.

163 Kolb (n 11) 7-9; Wolfrum, 'Sources of International Law' (n 2) 39.

164 ibid.

165 Kolb (n 11) 30; Wolfrum, 'Sources of International Law' (n 2) 39.

166 Wolfrum, 'General International Law' (n 2) 60.

167 Kolb (n 11) 30.

168 Bassiouni (n 3) 777ff.

(3.1), maintenance of international peace and security (3.2), and the duty to international cooperation in solving international problems (3.3), as well as their corollary principles, will be presented.

Importantly, after a respective concretisation in the context of cyberspace, these principles achieve the quality of legal ('hard law') rights or obligations of States. Furthermore, as general principles pertaining to international peace and security can be regarded as necessary for the 'co-existence and vital co-operation' within the international community, they will apply irrespective the States' practice, *opinio iuris*, consent or any other expression of will, and show a 'heightened' normativity from which States cannot decline (section 2.3).

3.1 Sovereign Equality of States and Corollary Principles

Sovereignty is the core notion of statehood and the axiomatic principle on which, in the words of the ICJ,[169] 'the whole of international law rests'.[170] It can be asserted that most, if not all principles of international law directly or indirectly rely on State sovereignty.[171] The principle is endorsed in Article 2(1) of the UN Charter in the form of an adjective ('sovereign equality') and ensures the juridical (not political, military, economic, geographic, demographic or other) equality of States.[172]

The understanding of sovereignty has undergone changes since its formal establishment in the Peace of Westphalia in 1648. Especially since 1945, its impact has been impaired by the recognition of international organisations (approximately 7,000) as subjects of international law and the acknowledgment of their decisions as a potential source of international law, by globalisation, the growing interdependence of States, and subsequent extended cooperation in fields which were formerly considered as domestic matters (approximately 50,000 international treaties are registered with the UN), by the recognition of rights of peoples (self-determination) as well as of individuals before specific international courts.[173] Furthermore, the notion of sovereignty is complemented by the understanding that States are obliged to promote and safeguard common values and goals of the international community.[174]

This is especially true with regard to cyberspace. The internet developed into a global network by a bottom-up, distributed effort of mainly private stakeholders. Cyberspace

169 Nicaragua (n 29) 263.

170 cf Heintschel von Heinegg (n 10) § 16 MN 43; Crawford (n 11) 447; Juliane Kokott, 'States, Sovereign Equality' in MPEPIL (n 2) MN 1; Brownlie (n 63) 287.

171 Samantha Besson, 'Sovereignty' in MPEPIL (n 2) MN 2; cf Epping and Gloria (n 143) § 26 MN 13.

172 d'Argent and Susani (n 105) 11.

173 cf Besson (n 171) 3-55, 153; Kokott (n 170) 79, 27; Bardo Fassbender, 'Die Souveränität des Staates als Autonomie im Rahmen der völkerrechtlichen Verfassung' in Heinz-Peter Mansel et al (eds), *Festschrift für Erik Jayme* (vol 2, Sellier 2004) 1093ff; idem (n 72) 69ff.

174 Fassbender (n 173) 1095.

(see definition in section 1), including its 'global public memory', is mainly driven by the civil society. The Westphalian elements of international order, i.e. of horizontal inter-State relations (emphasising the States as primary subjects of international law), are complemented in cyberspace in an extensive way by aspects of political, economic and social networks, characterised by vertical and diagonal linkages between governments, (transnational) companies, peoples, societies and individuals. The Internet Corporation for Assigned Names and Numbers (ICANN),[175] the non-governmental organisation (NGO) 'governing' the internet, can be deemed as reflecting this notion, as it takes an internationalised and multi-stakeholder approach to its operation.

Yet, although flexibly changing its nature, State sovereignty is still the foremost principle of international law and shows several significant facets and corollary principles, which will be presented in the following as applicable to cyberspace.

3.1.1 Self-Preservation

One of the corollary principles of equal sovereignty is a State's right to self-preservation. In its *Nuclear Weapons*[176] advisory opinion, the ICJ recognised 'the fundamental right of every State to survival, and thus its right to resort to self-defence, in accordance with Article 51 of the [UN] Charter, when its survival is at stake'. A right to self-defence is given in situations of an 'armed attack' launched by another State (or possibly by non-State actors), entitling the victim State to use defensive military force (Article 51 of the UN Charter and corresponding international custom[177]). Currently, neither a legal definition nor a universally accepted definition of the term 'armed attack' exists. It should be mentioned that State practice with regard to 'armed attacks' in the cyber context is not detectable and States prefer to maintain a strategic ambiguity with regard to the question as to under which circumstances they would consider malicious cyber activities as an 'armed attack', which leaves the respective discourse to academia.

175 ICANN is a Californian (US) non-profit, public benefit corporation, which, in the framework of a Public Private Partnership, acts on behalf of and reports to the US Department of Commerce (however, the organisation emphasises its international nature and independence). ICANN bears global responsibility for ensuring the stable and secure operation of the internet as well as for coordinating the internet system of unique identifiers, ie, for the assignment of IP address (see n 317) ranges (since 2005 to regional organisations). It is further responsible for the generic codes and country codes of the internet top level domain as well as for the management and maintenance of, as of 13 November 2013, the 386 internet root servers (which of location is secret), which are the backbone of the internet, see <http://www.root-servers.org/>. ICANN is contracted by the US Department of Commerce to perform the functions of the Internet Assigned Numbers Authority (IANA), which was executing the above-mentioned tasks directly on behalf of the US Department of Commerce. See ICANN, Factsheet <http://archive.icann.org/en/factsheets/fact-sheet.html>; ICANN / US Department of Commerce Contracts on IANA Functions <http://www.icann.org/en/about/agreements>.

176 *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion (1996) ICJ Rep 226, para 96.

177 Albrecht Randelzhofer and Georg Nolte, 'Article 51' in Simma (n 70) MN 10-12 (with further references); Karl Zemanek, 'Armed Attack' in MPEPIL (n 2) 14-21; Christopher Greenwood, 'Self-Defence' in MPEPIL (n 2) 1; Yoram Dinstein, *War, Aggression and Self-Defence* (3rd edn, Cambridge 2001) 165; Ian Brownlie, 'International Law and the Use of Force by States Revisited' (2000) 21 Australian Yearbook of International Law 21, 26; idem (n 63) 272-275.

In general terms, according to the ICJ and to scholarly writings, the notion of an 'armed attack' does not imply the use of specific weaponry, and can be thus conducted, for example, by electronic means.[178] Although disputed in detail, it can be asserted that an 'armed attack' is present in most severe cases of 'use of force' in international relations (Article 2(4) of the UN Charter) of significant scale and effects. This finding is supported by the jurisprudence of the ICJ[179] as well as by a vast amount of scholarly writings.[180] Thus, the question whether a situation of an 'armed attack' is present depends on the assessment whether a certain behaviour and their effects can be deemed as 'use of force' in the meaning of Article 2(4) of the UN Charter – a question which will be dealt with *infra* with regard to malicious cyber activities (section 3.2.1).

As cyberspace enables, skill and knowledge-wise, super-empowered individuals to cause severe physical effects through manipulations of computer systems that the functioning of highly developed post-industrial States depends upon, the question arises whether non-State actors can trigger the right to self-defence. There are considerable pros and cons for either approach, the demonstration of which would exceed the scope of this chapter.[181] In addition, the value of the so-called 'safe haven' theory,[182] developed in the context of self-defence with regard to terrorists acting from the territory of States unwilling or unable ('failed States') to impede activities of non-State actors harmful to other States, should be considered in the context of State responsibility for malicious cyber activities conducted by non-State actors otherwise qualifying as 'armed attack'. In this context, it would surely be beneficial to further discuss, e.g., the criteria of the terms 'unable' and 'unwilling' and the authority to determine their presence in a concrete case, as well as the nature of justifiable defence measures. An academic and political discourse on the aforementioned matters can probably not be avoided in the future.

178 Randelzhofer and Nolte (n 177) 43; Zemanek (n 177) 21; Nuclear Weapons (n 176) 39.

179 cf Nicaragua (n 29) 191, 195 ('the most grave forms', '[…] of significant scale […]', '[…] because of its scale and effects, would have been classified as an armed attack rather than a mere frontier incident […]'); *Oil Platforms*, Merits (2003) ICJ Rep 161, para 51, 64 and 72. With regard to the lawfulness of the use of armed force in cases of 'low intensity conflicts' see Randelzhofer and Nolte (n 177) 8.

180 cf Randelzhofer and Nolte (n 177) 4ff and 20; Zemanek (n 177) 7; Greenwood (n 177) 12; Michael Bothe, 'Völkerrechtliche Verhinderung von Gewalt (*ius contra bellum*)' in Wolfgang Graf Vitzthum (ed), *Völkerrecht* (De Gruyter 2001) section 8 para 10; Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford University Press 1994) 250.

181 cf eg Zemanek (n 177) 14-21; Michael N Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revised' (2011) 56 Villanova Law Review 569, 600ff; Katharina Ziolkowski, *Gerechtigkeitspostulate als Rechtfertigung von Kriegen. Zum Einfluss moderner Konzepte des Gerechten Krieges auf die völkerrechtliche Zulässigkeit zwischenstaatlicher Gewaltanwendung nach 1945* (NOMOS 2008) 221-229, demonstrating the lines of interpretation of Article 51 of the UN Charter, of the respective international customary law, as well as of international courts' jurisprudence, State practice and resolution practice of UN organs after the events of 9 September 2001. The Netherlands confirmed their view that non-State actors can conduct an 'armed attack' in cyberspace, see The Netherlands, 'Government response to the AIV/CAVV report on cyber warfare' (Statement of 17 January 2012) 5 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf>.

182 For an overview on the major lines of argumentation, see Schmitt (n 181) 602ff.

Furthermore, the 'accumulation of events' or '*Nadelstichtaktik*' theory will surely need to be considered within the cyber realm. The concept states that, in a situation of a series of incidents, of which each one classifies as 'use of [armed] force' but does not show the necessary scale and intensity qualifying it as an 'armed attack', the whole series of these occurrences would cumulatively form the basis for the assessment of the immediacy, scope and intensity. Advocates of this approach claim that a State facing a 'hit and run' tactic of another State would have no other choice but to undertake military measures to counter it.[183] In the past, the concept was invoked by Israel (using the term *Nadelstichtaktik*)[184] to justify the use of military force against terrorist groups located on the sovereign territory of its neighbouring States.[185] Furthermore, the US made use of the concept ('accumulations of events theory'),[186] e.g., to justify the bombardment of specific sites in Sudan and Afghanistan on 20-21 August 1998 in a letter to the UN Security Council (UNSC), stating:

> These attacks were carried out only after repeated efforts to convince the Governments of the Sudan and the Taliban regime in Afghanistan to shut these terrorist activities down and to cease their cooperation with Bin Ladin's organization. That organization has issued a series of blatant warnings that 'strikes will continue from everywhere' against American targets […]. The United States, therefore, had no choice but to use armed force to *prevent these attacks from continuing*. In doing so, the United States has acted pursuant to the *right of self-defence* confirmed by Article 51 of the Charter of the United Nations.[187]

Along these lines, some US and United Kingdom (UK) scholars view terrorist activities against the US as a continuous process.[188] Consequently, these scholars affirm that, due to the cumulative assessment of all terrorist activities, immediacy as well as a sufficient scope and intensity of an 'armed attack' is given at any time. Interestingly, the UNSC, including the US as a veto-power, clearly refused the rationale of the 'accumulation of events theory' by condemning on several occasions (until the 1970s) military

183 Dietrich Schindler and Kay Hailbronner, *Die Grenzen des völkerrechtlichen Gewaltverbots* (CF Müller 1986) 84; cf Nicaragua (n 29) 231 ('[…] incursions [...] amounting, singly or collectively, to an armed attack […]').

184 The term is used, eg, by Yehuda Zvi Blum, 'The Legality of State Response to Acts of Terrorism' in Benjamin Netanyahu (ed), *Terrorism. How the West Can Win* (Farrar, Straus and Giroux 1986) 133, 135.

185 Constantine Antonopoulos, *The Unilateral Use of Force by States in International Law* (A Sakkoulas 1997) 75.

186 Used first by the UNSC in 1953 during a meeting on military actions conducted by Israel against Libya, cf UN/SCOR 8th year, 637th meeting, para 4.

187 UN Doc S/1998/780 (20 August 1998) [emphasis added].

188 cf Christopher Greenwood, 'International Law and the "War Against Terrorism"' (2002) 78 International Affairs 301, 312; Rein Müllerson, '*Ius ad bellum* Plus Ca Change (de Monde) Plus C´est la M´me Chose (le Droit)?' (2002) 7 Journal of Conflict and Security Law 149ff; Sienho Yee, 'The Potential Impact of the Possible US Responses to the 9-11 Atrocities on the Law regarding the Use of Force and Self-Defence' (2002) 1 Chinese Journal of International Law 287, 292; Ruth Wedgwood, 'Responding to Terrorism: The Strikes Against bin Laden' (1999) 24 Yale Journal of International Law 559, 564.

actions justified on the basis of that theory (partly explicitly referring to such acts as 'retaliation').[189] On the contrary, the judgments of the ICJ in the *Nicaragua*[190] and *Oil Platforms*[191] cases indicate that the Court accepted the theory in general. However, the concept should be approached with caution. In the cyber context, only malicious cyber activities qualifying as 'use of [armed] force', and which – upon reliable information – will be followed with the utmost probability by other malicious cyber activities of the same quality, can be deemed as cumulatively amounting to an 'armed attack'.

Very likely, cases of preventive self-defence, i.e., in situations of an immediate 'armed attack', when '[…] the necessity of self-defence is instant, overwhelming, leaving no choice of means, and no moment for deliberation.',[192] will stay theoretical. This is based on the fact that, despite potential additional intelligence, the intended effect of malicious cyber activities will not be visible beforehand. Moreover, judged from today's perspective, even in the case of discovery of malicious codes in, for example, governmental computer networks, there still would be a 'choice of means' and a 'moment for deliberation'. Malware can be isolated, penetrated networks disconnected and IT security measures directed at the affected networks. Additionally, the concept of 'pre-emptive' (anticipatory) self-defence was asserted by some scholars, namely in the case of the implementation of the computer worm Stuxnet to Iranian nuclear facilities 2008-2010.[193] The concept of 'pre-emptive' self-defence, i.e., in cases of a mere suspicion of future armed attacks primarily based on mistrust towards a State's behaviour in international relations, is to be strictly refused[194] for several reasons, also regarding the

189 cf UNSC Res 101 (1953) (24 November 1953) part B para 1 and part A para 1 (Israel against Jordan); Res 111 (1956) (19 January 1956) preamble para 4, para 3 and 6 (Israel against Syria); Res 188 (1964) (9 April 1964) para 1 and 3 (UK against Arabic Republic Yemen); Res 265 (1969) (1 April 1965) preamble para 4, para 3 (Israel against Jordan).

190 Nicaragua (n 29) 146.

191 Oil Platforms (n 179) 64.

192 So-called 'Webster formula', phrased by the US State Secretary Webster in a letter to the British government of 24 April 1837, on the occurrence of the destruction of the US ship 'Caroline'; quoted by Brownlie (n 63) 43. On the 'Caroline Case' see Christopher Greenwood, 'Caroline, The' in MPEPIL (n 2).

193 See Michael N Schmitt (gen ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) Rule 13 para 13; contra: Katharina Ziolkowski, 'Stuxnet – Legal Considerations' (2012) 25 Journal of International Law of Peace and Armed Conflict (3) 143ff.

194 Greenwood (n 177) 47ff; Michael Bothe, 'Terrorism and the Legality of Pre-emptive Force' (2003) 14 European Journal of International Law 227, 230; Georg Nolte, 'Die USA und das Völkerrecht' (2003) 78 Friedens-Warte 119ff; Christian Tomuschat, 'Iraq – Demise of International Law?' (2003) 78 Friedens-Warte 141, 146; Rüdiger Wolfrum, 'The Attack of September 11, 2001, the Wars Against the Taliban and Iraq: Is There a Need to Reconsider International Law on the Recourse to Force and the Rules in Armed Conflict?' (2003) 7 Max Planck Yearbook of United Nations Law 1, 33; Ziolkowski (n 181) 235-240. See also *Case Concerning Armed Activities on the Territory of the Congo,* Judgement (2005) ICJ Rep 168, para 143 and 148. Contra: Olivier Corten, 'The Controversies Over the Customary Prohibition on the Use of Force. A Methodological Debate' (2005) 16 European Journal of International Law 802, 807; W Michael Reisman, 'Assessing Claims to Revise the Law of War' (2003) 97 American Journal of International Law 82, 87; Michael N Schmitt, 'Preemptive Strategies in International Law' (2003) 24 Michigan Journal of International Law 513, 534; Abraham D Sofaer, 'On the Necessity of Pre-emption' (2003) 15 European Journal of International Law 209, 210 and 214; Michael J Glennon, 'The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter' (2002) 25 Harvard Journal of Law and Public Policy 539, 552ff; Dinstein (n 177) 220.

specific case of Stuxnet.[195] Preventive measures against latent threats to international peace and security are within the decision-making authority of the UNSC (Article 39, 41-42 of the UN Charter).

It should be mentioned that the usual expectation of defence measures being conducted by a State's armed forces will probably not be met in the pure cyber context. Armed forces must develop and maintain defensive cyber capabilities in order to be able to defend their own networks (including the deployable components thereof), and thus to ensure their operability. They should develop offensive cyber capabilities as an additional military capability, enhancing the potential of precise, potentially non-lethal possibilities of interruption and disruption without necessarily causing physical damage outside of the targeted computer networks, i.e., to living beings or to objects. However, malicious cyber activities of a level which could be deemed as an 'armed attack' against a State will probably target critical infrastructure systems which, in technologically advanced States, are highly dependent on the availability and integrity of information and communication systems (ICTs), and which are in large part privately owned. In the case of a cyber 'armed attack' in the meaning of Article 51 of the UN Charter, e.g., against the banking system as such or the energy generation and distribution systems, only the internet service providers (ISPs) will notice irregular data streams (through monitoring of their network traffic sensors collecting information about the 'net flow', i.e., amount of routed data and their destination) and only the Computer Emergency Response Teams (CERTs) of the respective private companies will notice infections by malicious software (by monitoring of the intrusion detection/prevention systems conducting deep package filtering or by indications of malfunctioning of the facility's operations). At the same time, only these ISPs and CERTs will be able to deter such 'attacks' on a 'bit for bit' basis, as only they will have the possibility to block data streams or to undertake infection recovery activities based on the knowledge of the specific architecture, operating systems and adjustments the targeted complex computer systems show. Additionally, the defence against the actual 'armed attack' conducted by cyber means will most probably require recourse to the possibilities and capabilities of private cyber security companies or of companies which developed the targeted, specific, industrial IT systems or software, and which can provide 'patches' for the vulnerabilities used by the aggressor for penetrating the system in question. This will leave the actual conduct of the 'bit for bit' cyber defence measures to the industry, i.e., to the civil society as opposed to armed forces. The armed forces and other governmental entities can only support the industry in such endeavours, for example, by providing intelligence or other forms of assistance (apart from conducting measures such as kinetic defence to deter the armed attack). One of the consequences could be that, according to Article 51(3) of the Additional Protocol I of 1977 to the Geneva Conventions of 1949 (and respective customary law), the acting ISP and CERT

[195] cf Ziolkowski (n 193) 143ff.

personnel could lose the protection civilians enjoy against direct attack and become a legitimate military target (for the duration of actively defending the attacked networks). The existence of a (paramilitary) Estonian Defence League's Cyber Unit, the Austrian plan to establish a 'cyber militia' or 'voluntary cyber fire-brigades',[196] and respective considerations as currently addressed in Latvia reflect the endeavours of States to link private cyber defence capabilities to the government.

Additionally, it can be asserted that the fundamental right of States to self-preservation also entails the right to take protective measures in situations of necessity.[197] Necessity is given when essential interests of a State (or possibly of the international community as whole) are facing grave and imminent peril.[198] Under strict conditions, States may safeguard such interests by taking protective measures (see Article 25 of the ILC *Draft Articles on Responsibility of States for Internationally Wrongful Acts*).

3.1.2 Territorial Sovereignty and Jurisdiction

Another principle corollary to equal sovereignty of States is the principle of territorial sovereignty, including the principle of jurisdiction.[199]

The aspect of territorial sovereignty, i.e., the exercise of full and exclusive authority over a territory, protects physical components of the internet ('cyber infrastructure') that are located on a State's territory or are otherwise under its exclusive jurisdiction.[200] This includes any technical and other physical components located on the land territory, in internal waters, territorial sea, archipelagic waters, in national airspace or on platforms (e.g., vessels, aircraft or satellites).[201] The fact that the components of the internet are located on a State's sovereign territory but form, at the same time, part of the global internet, does not indicate a waiver of the exercise of such territorial jurisdiction.[202] On the contrary, a State cannot claim territorial sovereignty (or right to appropriation) with regard to the internet as a whole (that is, a global resource) or to cyberspace (that is, a common space).[203] Due to the global nature of the internet and cyberspace, this finding

196 cf 'Österreich überlegt Aufstellung einer „Freiwilligen Cyberwehr"' *Der Standard* (28 June 2012) <http://derstandard.at/1339639277027/Oesterreich-ueberlegt-Aufstellung-einer-Freiwilligen-Cyberwehr>.

197 cf Robin Geiß and Henning Lahmann 'Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention' in this volume, section 3.2.

198 See Ziolkowski (n 181) 285-331 on 'necessity' as a general principle of international law, which might exceed the notion of Article 25 ILC *Draft Articles on Responsibility of States for Internationally Wrongful Acts*.

199 cf Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace' in this volume.

200 Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012) 7, 10 and 13.

201 ibid 11.

202 cf Heintschel von Heinegg (n 200) 14.

203 cf ibid 9.

is not impaired by the fact that the internet is 'governed' by ICANN, which acts on behalf of and reports to the US Department of Commerce.

Territorial sovereignty is violated by any acts causing physical effects on another State's territory.[204] However, as indicated by the US,[205] who declared that it considered its (territorial) sovereignty as violated by 'disruption of networks and systems', i.e., including intrusions without (directly or indirectly) showing a physical effect, it could be argued that physical damage is irrelevant in the cyber context.[206] Indeed, due to the enormous negative effects malicious cyber activities can have on the national security of another State, which can be, although not of physical nature, though well 'perceptible' (e.g., disruption of a State's – digital – stock exchange system), it can be claimed that such effects could violate the victim State's sovereignty.

The principle of jurisdiction describes the power of a State to define and to enforce rights and duties, and to control the conduct of natural and juridical persons (primarily on its own territory).[207] A State exercises its jurisdiction by establishing rules (legislative jurisdiction), procedures for identifying breaches of the rules and the precise consequences thereof (judicial jurisdiction), and by forcibly imposing consequences (enforcement jurisdiction).[208]

The general access to the internet (or digitalised access to information) can be deemed as protected by the universal human right to seek, receive and impart information through any media (see Article 19(1) of the *International Covenant on Civil and Political Rights* of 1966, Article 10(1) of the *European Convention on Human Rights* of 1950). However, a State may regulate internet activities of its own (nationality principle) and foreign (territoriality principle) nationals in its territory (or those conducted on foreign territory but showing effects on its own territory),[209] e.g., with regard to contents of uploads or downloads, including questions of what is deemed offensive in terms of morality, security and stability.[210]

The principle of jurisdiction would certainly be violated by law enforcement activities[211] (i.e., exercise of authority) conducted by foreign agencies in networks and computers located on a State's territory and outside of a cooperation framework or otherwise

204 cf ibid 11ff, 16; Lawrence T Greenberg, Seymour E Goodman and Kevin J Soo Hoo, *Information Warfare and International Law* (US National Defence University 1998) 24; similar: Christopher C Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 European Journal of International Law 825, 843.

205 The President of the United States of America, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (May 2011) 4 [call-out-box, 'Defence Objective'].

206 Similarly, in the context of territorial sovereignty Heintschel von Heinegg (n 200) 11ff.

207 Bernard H. Oxman, 'Jurisdiction of States' in MPEPIL (n 2) MN 3.

208 ibid.

209 ibid 32.

210 ibid 31; similarly Heintschel von Heinegg (n 200) 9, 14ff.

211 cf Oxman (n 207) 47.

without a prior consent of the territorial State (e.g., online search). Especially with regard to cyber crime law enforcement, the exercise of jurisdiction of States may overlap due to the competing territorial, personal and effects based facets of jurisdiction, additionally complicated by the mobility of users and technological advances such as cloud-based computing. These aspects call for intensified cooperation measures in cyber crime law enforcement.

3.1.3 Non-intervention in Domestic Affairs

A further principle deriving from the sovereign equality of States is the principle of non-intervention in the internal or foreign affairs of another State.[212] It is endorsed in regional conventions (e.g., Articles 16-19 of the *Charter of the Organisation of American States*, Article III(2) of the *Charter of the Organization of African Unity*), reflected in political declarations (e.g., Principle VI of the *Helsinki Final Act* of 1975)[213], in UNGA resolutions,[214] and is endorsed in Article 2(7) of the UN Charter (with regard to UN organs). The principle is confirmed by the ICJ as a rule of international custom.[215] An illegal intervention occurs when a State interferes with the internal or external affairs of another State considered by the latter as 'internal' or 'domestic' (*domaine réservé*), in order to coerce the other into certain behaviour.[216]

In general terms, it can be asserted that *domaine réservé* describes areas not regulated by international norms or not being of some common interest or value.[217] Due to globalisation, the integration of States in international organisations, the growing interdependence and subsequent cooperation of States, and especially the myriad of conventional law, very few matters can nowadays be regarded as remaining within the limits of purely 'domestic jurisdiction'.[218] One of the matters which are still recognised as *domaine réservé*, although significantly internationalised by human rights law, is the

212 cf Terry D Gill, 'Non-Intervention in the Cyber Context' and Chris Demchak, 'Economic and Political Coercion and a Rising Cyber Westphalia' in this volume.

213 n 74.

214 eg *Friendly Relations Declaration* (n 71) Principle 1; *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty* UNGA Res 2131 (XX) (21 December 1965) para 2; *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States* UNGA Res 36/103 (9 December 1981) para 2, Principle I(b) and II(a); *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations* UNGA Res 42/22 (18 November 1987) annex para 8.

215 Corfu Channel (n 29) 35; Nicaragua (n 29) 202.

216 Nicaragua (n 29) 202ff; Philip Kunig, 'Intervention, Prohibition of' in MPEPIL (n 2) MN 1.

217 Kunig (n 216) 3; Ulrich Beyerlin, 'Intervention' in Rüdiger Wolfrum and Christiane Philipp (ed), *United Nations: Law, Policies and Practice* (vol I, CH Beck 1995) para 7; cf Georg Nolte ,'Article 2(7)' in Simma (n 70) MN 27; Katja S Ziegler, 'Domaine Réservé' in MPEPIL (n 2) MN 1; d'Argent and Susani (n 105) 18.

218 Kunig (n 216) 3; cf Fassbender (n 72) 70; Nolte (n 217) 27. Ziegler considers the impact of *domaine réservé* as 'more symbolic than legal', Ziegler (n 217) 32.

jurisdiction over, and the regulation and treatment of own and foreign nationals.[219] So far, the deliberations as presented above apply (section 3.1.2).

The internet communication as such (as opposed to national intranets) cannot be deemed as an internal affair of a State, as international telecommunications are regulated by international law (Articles 33-48 of the *Constitution of the International Telecommunication Union* (ITU Constitution), e.g., with regard to denial or restriction of internet connectivity). Additionally, due to the nature of the internet as a globally shared resource and to the – in general – worldwide spread of malicious software, aspects of national cyber security, i.e., questions of the establishment of cyber security measures of a strategic, political, legal, administrative, organisational and technical nature, including the establishment of a national CERT, must be deemed as of internationalised interest or value, and thus outside of the realm of purely internal affairs.

In order to violate the non-intervention principle, 'coercion', as opposed to perfectly legal (political, economic, etc.) influence, must be employed.[220] The meaning of the term is unclear.[221] Scholars assert that illegal coercion implies massive influence, inducing the affected State to adopt a decision with regard to its policy or practice which it would not envision as a free and sovereign State.[222] The *Friendly Relations Declaration* (Principle 3) describes armed intervention, obtaining subordination of the exercise of a State's sovereign rights, and actions directed towards the violent overthrow of a regime of another State, as violating the non-intervention principle. This results in the notion that 'coercion' occurs only in drastic cases of overwhelming (direct or indirect) force being put upon a State's free and sovereign decision-making process.

Thus, it is not probable that, for example, online law enforcement activities of foreign agencies (see section 3.1.2) would be considered by the affected State as meeting the threshold of impact as required by the notion of 'coercion'. The question of access to the internet or demands for the establishment of a national cyber security framework can surely not be deemed as violating the non-intervention principle, as such matters cannot be categorised as purely internal affairs of a State.

3.1.4 Duty Not To Harm Rights of Other States (Principle of Prevention, Precaution and 'Due Diligence')

Another principle aiming to de-conflict equal sovereignties of States is the duty not to harm the rights of other States and consequently, as confirmed by the ICJ,[223] not to let its own sovereign territory be used for activities causing damage to persons or objects

219 Ziegler (n 217) 5.

220 See discussion at Kunig (n 216) 5ff.

221 ibid. The *Friendly Relations Declaration* also preserves a vague wording in this regard, see Keller (n 72) 20ff.

222 Kunig (n 216) 22-27; Beyerlin (n 217) 809.

223 Corfu Channel (n 29) 22.

protected by the sovereignty of another State (see also Article 1(2) of the UN Charter, endorsing a 'principle of equal rights').[224] The principle is closely related to the principle of good neighbourliness and the supporting maxim (or normative rule) *sic utere tuo ut alienum non laedas* (use your own property so as not to harm that of another), which are discussed *infra* (section 3.1.5) in more detail.

The no-harm principle includes the obligation of States to take preventive measures in concrete cases of risk of harm to other States' rights, of which the State in question has knowledge or presumptive knowledge.[225] Such an obligation can be derived from the logic of the no-harm obligation, and can be deemed as confirmed by the ICJ in the *Hostages*[226] case (referring to preventive duties deriving from conventional and customary diplomatic law), and in the *Nuclear Weapons*[227] advisory opinion. It is endorsed in a multitude of treaties concerning environmental protection, nuclear accidents, space objects, international watercourses, management of hazardous waste, and prevention of marine pollution.[228] An obligation to prevention is further enshrined in Article 3 of the ILC *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*[229] of 2001, which states: 'The State […] shall take all appropriate measures to prevent significant transboundary harm [to the environment, persons or property] or at any event to minimize the risk thereof.'

According to the draft articles, such measures comprise, for example:

- risk assessment (Article 7),
- notification and information in cases of risk of causing significant transboundary harm (Article 8), and
- consultation on preventive measures (Article 9).

These procedural duties are nowadays widely recognised as being part of international law, either in the form of international custom or of general principles of international law.[230] As Article 1 of the aforementioned draft indicates, these obligations might refer only to risk of harm of physical nature. However, it could be argued that non-physical, though well perceptible, damage is relevant in the cyber context (section 3.1.2).

---

224 cf Heintschel von Heinegg (n 200) 7ff, 16 (with references).

225 eg ibid; Epping and Gloria (n 143) § 26 MN 16.

226 Hostages (n 93) 68.

227 Nuclear Weapons (n 176) 29.

228 ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities,* with commentaries (2001) UN Doc A/56/10, General commentary, para 3 <http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf>; cf references at Philippe Sands, *Principles of International Environmental Law* (2nd edn, Cambridge University Press 2003) 246ff.

229 See supra n 228.

230 Günther Handl, 'Transboundary Impact' in Daniel Bodansky, Jutta Brunnée and Ellen Hey (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007) 531, 541 (with further references).

Furthermore, it can be attested that States are also obliged to take (general) precautionary measures with regard to potential cyber threats posing a significant risk of damage of a transboundary nature. The precautionary principle forms the basis of the legal regimes governing the high seas (*The United Nations Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks* of 1995) and Antarctica (*Protocol on Environmental Protection to the Antarctic Treaty* of 1991). Additionally, it is enshrined in several international treaties on environmental protection,[231] and is pronounced as either evolving[232] or already existing[233] customary rule of international environmental law.

As described above, it is certified by international courts and by scholarly writings that general principles of international law can, *inter alia,* be identified by deduction from the legal logic and from specific legal regimes or treaty regimes (see section 2.1). Once the existence of a general principle of international law is established in such a manner, and showing openness for concretisation in other circumstances, it can be applied to other situations or areas.[234] Such a technique does not present an analogy[235] (i.e., creation of new rules in cases of legal *lacuna*, by treating similar cases the same way legally)[236] in *sensu stricto*.[237] It should be mentioned that, due to the fact that the internet is another global resource beside the natural environment, and cyberspace is another common space beside the high seas and Antarctica, and that the area is sparsely regulated (especially the ITU rules on international telecommunications do not entail cyber security regulations), an analogy would, in theory, seem not to be far-reaching. A common feature and overarching principle of the above-mentioned treaty regimes for globally shared resources and common spaces is the obligation to take precautionary measures. Such a principle is open for concretisation in other situations, and can subsequently be applied to the internet as another globally shared resource, and to cyberspace as another common space.[238]

231 cf discussion and references at Sands (n 228) 266-279.

232 ibid 279; Winfried Lang, 'UN-Principles and International Environmental Law' (1999) 3 Max Planck Yearbook of United Nations Law 157, 167.

233 Ulrich Beyerlin and Jenny Grote Stoutenburg, 'Environment, International Protection' in MPEPIL (n 2) MN 24.

234 Heintschel von Heinegg (n 10) § 19 MN 7.

235 The use of a legal rule in an analogous way (*per analogiam*) means the application of a rule which covers a particular case to another case which is similar to the first but itself not regulated by the rule. See Silja Vöneky, 'Analogy in International Law' in MPEPIL (n 2) MN 1.

236 ibid 4ff.

237 Heintschel von Heinegg (n 10) § 19 MN 6ff.

238 The application of principles of environmental law to the internet/cyberspace was first proposed by Torsten Stein and Thilo Marauhn, 'Völkerrechtliche Aspekte von Informationsoperationen' (2000) 60 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 1, 21.

Taking another conceptual approach, it was proposed in diplomatic circles (and is claimed by the US[239] to be an 'emerging norm') to introduce a principle of 'due diligence'[240] of States (by a broad interpretation of the no-harm rule) with regard to malicious cyber activities of non-State actors originating from the States' territories and harming rights of other States. Given that all States acknowledge the relevance of malicious cyber activities for national and international peace and security, as shown by the multitude of respective UNGA resolutions,[241] including the establishment of all in all six GGEs[242] on diverse cyber challenges, and by the adoption of Organisation for Economic Co-operation and Development (OECD) *Guidelines for the Security of Information Systems*[243] of 1992, it can be held that, assuming the thus confirmed common interest of States in cyber security, the duty to prevention could exceed concrete cases and be interpreted in general terms of 'due diligence' (similar to the 'precautionary principle' as a general principle of international law applicable in to the internet and to cyberspace). Some scholarly writings assert that cyber security 'due diligence' is already part of international custom.[244]

239 The President of the United States of America (n 205) 10.

240 cf Robin Geiß and Henning Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention' in this volume.

241 cf *Developments in the field of information and telecommunications in the context of international security* UNGA Res 53/70 (4 December 1998), 54/49 (1 December 1999), 55/28 (20 November 2000), 56/19 (29 November 2001), 57/53 (22 November 2002), 58/32 (8 December 2003), 59/61 (3 December 2004), 60/45 (8 December 2005), 61/54 (6 December 2006), 62/17 (5 December 2007), 63/37 (2 December 2008), 64/25 (2 December 2009), 65/41 (8 December 2010), 66/24 (2 December 2011), 67/27 (3 December 2012);
Creation of a global culture of cybersecurity, UNGA Res 57/239 (20 December 2002) (proposing nine elements for creating a global culture of cybersecurity, annex), *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* UNGA Res 58/199 (23 December 2003) (proposing eleven elements for protecting critical information infrastructures, annex), and *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, UNGA Res 64/211 (21 December 2009) (proposing 'voluntary self-assessment tool for national efforts to protect critical information infrastructure' of 18 points, annex);
see also UNGA Res 55/63 (4 December 2000) and 56/121 (19 December 2001) (combating the criminal misuse of information technologies), 57/239 (20 December 2002) (creation of a global culture of cybersecurity) and 58/199 (23 December 2003) (creation of a global culture of cybersecurity and the protection of critical information infrastructures), 64/211 (21 December 2009) (creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures), 55/63 (22 January 2001) and 56/121 (23 January 2002) (combating the criminal misuse of information technologies), and UNGA Res 63/195 (18 December 2008), 64/179 (18 December 2009), and 65/232 (21 December 2011) (strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular, its technical cooperation capacity). The Third Committee deferred considerations on the subject on the criminal misuse of information technologies, pending work of the Commission on Crime Prevention and Criminal Justice, UNGA Res 56/121 (23 January 2002, para 3).

242 For details see Katharina Ziolkowski, 'Confidence Building Measures for Cyberspace' in this volume, section 3.3.1.

243 The guidelines call for cooperation of States (Principle 6) in the area of 'comprehensive protection' of information systems (Principle 4), and stipulate an imperative of deliberation in the use of information systems (Principle 3), OECD Doc OCDE/GD(92)190.

244 Heintschel von Heinegg (n 200) 18.

The concrete features of preventive and precautionary (or the proposed 'due diligence') measures would stay within the discretion of the States.

However, the prevention principle obliges States to undertake a risk assessment and to inform, notify, and consult other States in concrete cases of risk of significant transboundary harm. This preconditions the ability of a State to notice irregular data streams or malicious software as such. This results, as a minimum, in the obligation of States to ensure (1) that the national ISPs install network sensors collecting information on 'net flow', i.e., amount of routed data and their destination (allowing the detection of, e.g., 'DDoS attacks'), (2) that national tier 1 ISPs install intrusion detection/prevention systems at their 'gates' of international data transmission and conduct deep package filtering (allowing recognition of malicious software), and (3) that an obligatory reporting system to a governmental entity (e.g., a national or governmental CERT) with regard to significant cyber incidents is in place. Furthermore, the conduct of the above-described measures, the procedural obligations of notification, information and consultation, as well as the general management of the prevention of malicious cyber activities potentially harming other States' rights, require the establishment of a framework of strategic, political, legal, administrative, organisational and technical nature. Additionally, the preventive principle would also oblige a State to establish investigative cyber capabilities (allowing the identification of the source of the malicious cyber activities) either within a CERT, the police, or other security forces, depending on the division of responsibilities and authorisations pertaining to respective national laws (either existing or to be endorsed), as well as the organisational and legal framework allowing the prevention or discontinuation of concrete malicious cyber activities originating on the State's territory and potentially harming the rights of other States.

The precautionary principle (as well as the proposed 'due diligence' principle) includes the duty to undertake all appropriate regulatory and other measures at an early stage, and well before the (concrete) risk of harm occurs.[245] This would involve the implementation of strategic, political, organisational, administrative, legal and technical measures (including the above-mentioned measures) aimed at general prevention of the misuse of the possibilities that cyberspace offers for respective malicious activities by non-State actors, i.e., the establishment of a national cyber security framework[246]. Such an obligation would apply only with regard to cyber activities possibly violating the rights of other States, thus inflicting severe damage (even if of a non-physical nature), i.e., with regard to cyber threats which can be deemed as clearly affecting other States' national security.[247] The specification of which malicious cyber activities would clearly

245 Sands (n 228) 246ff.

246 On national cyber security framework see Alexander Klimburg (ed), *National Cyber Security Framework Manual* (NATO CCD COE Publication 2012).

247 Similarly: Heintschel von Heinegg (n 200) 16 (excluding cyber espionage and other 'mere intrusions into foreign computers or networks').

affect the national security of States must be left to future State practice. It can be only assumed that, due to the interests of States, espionage activities would not fall under this category.[248] Nonetheless, the acknowledgement of the precautionary principle (or 'due diligence') for cyberspace entails the obligation to set up a national cyber security framework with regard to respective cyber threats (including these going beyond causing possible physical harm).

It should be mentioned that, as stated above (section 3.1.3), demands for the establishment of a national cyber security framework (including the technical aspects thereof) cannot be deemed as a forbidden intervention in domestic affairs, as, due to the global nature of cyberspace and the internet, questions of cyber security do not fall under the category of purely internal matters.

3.1.5 Principle of Good Neighbourliness and *sic utere tuo*

Furthermore, balancing the competing sovereign rights of States, the principle of good neighbourliness has a relevance to cyberspace. The principle needs to be distinguished from the 'international law of neighbourliness' governing the relations of neighbouring States only in the frontier zones of their territories.[249] The principle of good neighbourliness is endorsed in a legally binding manner in the preamble of the UN Charter (whereas Article 74 refers to 'general principle of good-neighbourliness [...]' as a binding aim for policies with regard to colonies).[250] Moreover, the principle is endorsed as a legal obligation in international environmental law (especially referring to the use of trans-border resources such as rivers).[251] The principle mutually limits the sovereign exercise of activities potentially affecting neighbours in an intolerable manner, and is confirmed by the maxim (or normative rule) of *sic utere tuo ut alienum non laedas* (use your own property so as not to harm the one of another).[252] From the principle of good neighbourliness derive the obligations:[253]

- not to use or permit to use the territory in a manner as to cause damage to the territory of neighbouring States (see also section 3.1.4),
- to adopt any necessary – preventive and precautionary – measures in order to avoid or reduce damage beyond the own territory,

248 ibid, though based on other deliberations. On espionage see Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in this volume.

249 Laurence Boisson de Chazounes and Danio Campanelli, 'Neighbour States' in MPEPIL (n 2) MN 6-8.

250 Ulrich Fastenrath, 'Article 74' in Simma (n 70) MN 2.

251 ibid 2; cf Boisson de Chazounes and Campanelli (n 249) 18-20.

252 Boisson de Chazounes and Campanelli (n 249) 10; Jutta Brunnée, 'Sic utere tuo ut alienum non laedas' in MPEPIL (n 2) MN 1, 15ff.

253 Boisson de Chazounes and Campanelli (n 249) 11.

- to inform, notify, consult neighbours on any situation likely to cause damage beyond own territory,
- to tolerate activities otherwise not prohibited under international law so long as the consequences do not exceed an acceptable threshold of gravity (specified on a case-to-case basis).

As the principle of good neighbourliness had already been introduced to other types of vicinity than frontier regions (e.g., to contiguous and exclusive economic zones on the high seas or to 'regions'),[254] a further extension to cyberspace seems justified due to its global nature, to the speed and density of the internet connections and to its importance for inter-State relations of political, economic and other nature; aspects creating as a whole a modern form of 'vicinity'. This view can be deemed as confirmed by the UNGA, which recognised already in 1991 that 'great changes of political, economic and social nature, as well as the scientific and technological advances that have taken place in the word and led to unprecedented interdependence of nations, have given new dimensions to good-neighbourliness [...]', and emphasised that all States shall act as good neighbours 'whether or not they are contiguous'.[255]

However, the above-mentioned obligations deriving from the principle of good neighbourliness refer to physical damage only, a finding which can be considered as confirmed by Article 1 of the aforementioned ILC *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*. As stated above, it could be suggested that the aspect of physical damage is irrelevant in the cyber context (section 3.1.2). Due to the enormous negative effects malicious cyber activities can have on the national security of another State it can be claimed that also harm of non-physical nature, though relevant to national security of another State, is governed by the principle of good neighbourliness.

This finding, comparable to the obligations deriving from the precautionary principle or from a potential 'due diligence' principle (see section 3.1.4), invokes the obligations of States to take preventive and precautionary measures (i.e., enhancing national cyber security) with regard to respective cyber threats, as well as obligations to inform, notify, and consult in concrete cases of risk of significant transboundary harm.

3.2 Maintenance of International Peace and Security

Maintenance of international peace and security is the paramount purpose of the UN, enshrined in Article 1(1) of its Charter.[256] According to a systematic interpretation of the Charter, as well as according to the UNGA *Friendly Relations Declaration* and the

254 ibid 12.

255 UNGA Res 46/62 (9 December 1991) preamble, para 3 and operative section, para 2.

256 d'Argent and Susani (n 105) 4.

Proclamation of the International Year of Peace[257] of 1985, peace is not understood negatively, as an absence of (declared) war or of any other international armed conflict, but has become 'multidimensional',[258] requiring a series of active actions, taken collectively by States and peoples, reaching, *inter alia,* from the removal of various threats to peace and security to the development of confidence building measures.[259] The general principles of international law corollary to this aim are the duty to refrain from threat or use of force in international relations (3.2.1) and the closely related duty to peaceful settlement of international disputes (3.2.2), both being the foremost means of prevention of (declared) war or of any other international armed conflict.[260]

3.2.1 Refrain from Threat or Use of Force in International Relations

The prohibition of threat or use of force in international relations constitutes one of the cornerstones of the international legal order.[261] The principle is endorsed in Article 2(4) of the UN Charter and is (in its core) widely considered as a peremptory norm of international custom.[262] According to the systematic, historical and teleological interpretation of the UN Charter, as well as pursuant to the jurisprudence of the ICJ and scholarly writings, the term 'force' is to be understood as 'armed force'.[263] The term 'use of [armed] force', however, is not limited to the employment of military weaponry in the common sense of the term.[264] The ICJ attested over 25 years ago in its *Nicaragua*[265] judgement the possibility of an 'indirect' or non-military use of armed force (e.g., by arming and training insurgents) and scholarly writings describe, for example, spreading fire over the border or flooding another State's territory as violating the prohibition of 'use of [armed] force'.[266]

In order to specify the meaning of 'use of [armed] force' conducted by means of the internet or other ICT systems, an effects-based approach inherent to public international

257 UNGA Res 40/3 (24 October 1985).

258 d'Argent and Susani (n 105) 25.

259 ibid 7; Rüdiger Wolfrum, 'Article 1' in Simma (n 70) MN 9ff. cf Katharina Ziolkowski, 'Confidence Building Measures for Cyberspace' in this volume.

260 Albrecht Randelzhofer and Oliver Dörr, 'Article 2(4)' in Simma (n 70) MN 2.

261 ibid 1; Oliver Dörr, 'Use of Force, Prohibition of' in MPEPIL (n 2) 1; cf Nicaragua (n 29) 190 ('fundamental or cardinal principle of […] [customary international] law').

262 Randelzhofer and Dörr (n 260) 64-68; Dörr (n 261) 1, 10, 32; Wolfrum, 'General International Law' (n 2) 45; d'Argent and Susani (n 105) 23; Ziolkowski (n 181) 200-205 (with further references); Nicaragua (n 29) 100. See scepticism due to contrary State practice at Michael J Glennon, *Limits of Law, Prerogatives of Power: Interventionism after Kosovo* (Basingstoke 2001) 44, 56; idem, 'Why the Security Council Failed' (2003) 82 Foreign Affairs (3) 16, 23ff.

263 cf Dörr (n 261) 11; Marco Roscini, 'World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force' (2010) 14 Max Planck Yearbook of United Nations Law 85, 104-106; see also Randelzhofer and Dörr (n 260) 16-20; Thomas Bruha, 'Use of Force, Prohibition of' in Wolfrum and Philipp (n 217) 1387ff.

264 Randelzhofer and Dörr (n 260) 21; Dörr (n 261) 12 (referring explicitly to cyber means).

265 Nicaragua (n 29) 228.

266 Randelzhofer and Dörr (n 260) 21; Dörr (n 261) 12.

law is appropriate (ruling out other possible approaches, e.g., focusing on the target of the malicious activities, the intent of the malevolent actor, or the categorisation of the means used).[267] Hereby, a comparison of the effects indirectly caused or intended by malicious cyber activities with the effects usually caused or intended by conventional, biological or chemical weapons (BC weapons) is necessary.[268] According to the traditional understanding, 'use of [armed] force' requires the employment of kinetic weaponry, i.e., of a tool designed to cause kinetic effects of a physical nature on a body or on an object. The transfer of data and its delay or interruption, as well as the manipulation, suppression or deletion of data cannot be deemed to cause (directly) kinetic effects in the common meaning of the term. In contrast, some similarities between malicious cyber activities and BC weapons can be conceived. The use of BC weapons does not cause destruction in the conventional sense, as these weapons do not release kinetic energy.[269] The employment of BC weapons is considered as a form of 'use of [armed] force' because they can cause death or injury to living things.[270] Thus, in the case of BC weapons, the term 'weapon' is defined with reference to their effects rather than their method, which perfectly corresponds with the effects-based approach inherent to public international law. Consequently, the majority of scholars rightly insist on an effects-based interpretation of the term of 'use of [armed] force' in the cyber context.[271] Therefore, it can be assumed that malicious cyber activities can be considered 'use of [armed] force' in the meaning of Article 2(4) of the UN Charter if they – indirectly – result in:[272]

- death or physical injury to living beings and/or the destruction of property,[273]
- massive, medium to long-term disruption of critical infrastructure systems of a State (if in its effect equal to the physical destruction of the respective systems).[274]

267 Similar Randelzhofer and Dörr (n 260) 22.

268 cf Randelzhofer and Nolte (n 177) 43.

269 Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 New York University Journal of International Law and Politics 57, 72; Todd A Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 Case Western Reserve Journal of International Law 567, 590.

270 Brownlie (n 63) 362.

271 Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law (3) 885, 913 and 919; Stein and Marauhn (n 238) 6.

272 For detailed discussion see Katharina Ziolkowski, 'Computer Network Operations and the Law of Armed Conflict' (2010) 49 Military Law and the Law of War Review 47, 69-75.

273 Randelzhofer and Nolte (n 177) 43; Yoram Dinstein, 'Computer Network Attack and Self-Defense' in Michael N Schmitt and Brian T O'Donnell (eds), *Computer Network Attack and International Law* (US Naval War College 2002) 99, 103; Daniel B Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' in Schmitt and O'Donnell (supra) 73, 85; Barkham (n 269) 80; Stein and Marauhn (n 238) 7; Joyner and Lotrionte (n 204) 850; Walter G Sharp, *Cyberspace and the Use of Force* (Aegis Research Cooperation 1999) 102; Schmitt (n 271) 914ff; Morth (n 269) 591; Greenberg, Goodman and Soo Hoo (n 204) 19 and 32.

274 Randelzhofer and Nolte (n 177) 43; Ziolkowski (n 272) 69-75; James P Terry, 'Responding to Attacks on Critical Computer Infrastructure. What Targets? What Rules of Engagement?' in Schmitt and O'Donnell (n 273) 421,

In contrast, neither the mere destruction of data (even of substantial importance, e.g., classified data, or of significant economic value, e.g., symbolising assets)[275] nor the 'theft'[276] (rather, illegal copying) of data (being nothing more than modern espionage[277] neither generally permitted nor forbidden under public international law) can be considered 'use of [armed] force'.[278] Such effects cannot be equated to the effects usually caused or intended by conventional or BC weapons, especially not to the physical destruction of objects.[279]

'Use of [armed] force' in the meaning of Article 2(4) of the UN Charter is to be distinguished especially from measures of mere (economic or political) coercion in international relations, a task that can pose considerable challenges upon decision-makers in practice. For facilitating such a distinction, in 1999[280] Professor Schmitt developed and recently reinforced[281] a set of criteria for the determination of 'use of [armed] force' (amending their descriptions over time), namely severity, immediacy, directness, invasiveness, measurability, presumptive legality (earlier: legitimacy) and responsibility.[282] The factors shall serve as indicators which States are likely to take into consideration when assessing whether specific malicious cyber activities qualify as 'use of [armed] force'.[283] However, they are not meant as legal criteria.[284]

428ff; Morth (n 269) 599; Sharp (n 273) 129ff. Contra: Michael N Schmitt, 'The 'Use of Force', in 'Cyberspace: A Reply to Dr Ziolkowski' in Czosseck, Ottis, Ziolkowski (n 200) 311, 315; Dinstein (n 273) 105; Stein and Marauhn (n 238) 8, who demand the occurrence of physical damage outside the targeted computer networks in order to qualify CNO as use of force.

275 cf Michael N Schmitt, Heather A Harrison Dinniss and Thomas C Wingfield, *Computers and War: The Legal Battlespace* (International Humanitarian Law Research Institute, Background Paper 2004) 5ff; Barkham (n 269) 88.

276 Joyner and Lotrionte (n 204) 855ff; contra: Stein and Marauhn (238) 10.

277 Anthony D'Amato, 'International Law, Cybernetics, and Cyberspace' in Schmitt and O'Donnell (n 273) 59, 67; Stein and Marauhn (n 238) 32 (with further references). With regard to cyber activities as modern form of espionage, cf Wolff Heintschel von Heinegg, 'Informationskrieg und Völkerrecht. Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung' in Volker Epping, Horst Fischer and Wolff Heintschel von Heinegg (eds), *Brücken bauen und begehen. Festschrift für Knut Ipsen zum 65. Geburtstag* (CH Beck 2000) 129, 134. Apart from the penalisation of espionage resulting from respective national law systems, spying is restrained by certain provisions of public international law, eg, the taboos stated by the diplomatic and consular law protecting diplomatic and consular archives and correspondence, ie, respective electronic databases and internet communication; cf Jovan Kurbalija, 'E-Diplomacy and Diplomatic Law in the Internet Era' and Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in this volume.

278 Ziolkowski (272) 69-75.

279 cf ibid for detailed discussion.

280 Schmitt (n 271) 913ff.

281 idem (n 181) 576ff (the criterion of 'responsibility' was mentioned already in the 1999 publication, although only in a footnote, see idem (n 271) 915, footnote 81).

282 ibid 576ff.

283 ibid 605.

284 Schmitt (n 274) 314; see also discussion of the criteria at Katharina Ziolkowski, '*Ius ad bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force' in Czosseck, Ottis, and Ziolkowski (n 200), 295-309.

State practice and *opinio iuris,* apart from a political declaration of the US[285] to respond to 'hostile acts in cyberspace' with self-defence measures, is hitherto not detectable. Although States in general prefer to maintain a strategic ambiguity with regard to questions related to use of force, thus leaving the debate to academia, it would certainly support predictability and thus stability in international relations, if they shared their views on this aspect.

3.2.2 Peaceful Settlement of Disputes

The legal[286] obligation to peaceful settlement of international disputes is endorsed in Article 2(3) of the UN Charter, specified by the UNGA in its *Friendly Relations Declaration* as well as in the *Manila Declaration on the Peaceful Settlement of International Disputes*[287] of 1982, and recognised by the ICJ as a 'principle of customary international law.'[288]

The principle limits the notion of sovereignty and correlates to the principle of the prohibition of threat or use of force in international relations, recognising that unsettled disputes can lead to eruptive disturbances within the international community.[289] The dispute in question does not need to endanger international peace and security (see on the other hand Article 33-38 of the UN Charter). The pacific means of dispute resolution consist of diplomatic-political measures (e.g. negotiation, inquiry, mediation, conciliation) and legal measures (arbitration and litigation) (compare Article 33(1) of the UN Charter).[290] Although no compulsory instrument of adjudication exists, the majority of scholars deem the principle as establishing an obligation to deploy active efforts to settle international disputes (in the meaning of conduct, not outcome).[291] With regard to the means of peaceful settlement of international disputes, States have a wide-ranging discretion, although the UN Charter contains some proposals in its Chapter VI concerning disputes endangering international peace and security (including investigative powers of the UNSC and the possibility to bring a dispute to the attention of the UNGA or the UNSC).[292]

A violation of the principle can only be affirmed if a party to an international dispute constantly refuses to even attempt to reach a settlement.[293] Thus, in cases of

285 The President of the United States of America (n 205) 12ff. and 14.

286 cf Christian Tomuschat, 'Article 2(3)' in Simma (n 70) MN 23; Wolfrum, 'General International Law' (n 2) 44.

287 UNGA Res 37/10 (15 November 1982).

288 Nicaragua (n 29) 290.

289 Tomuschat (n 286) 2; d'Argent and Susani (n 105) 13.

290 Anne Peters, 'International Dispute Settlement: A Network of Cooperational Duties' (2003) 14 European Journal of International Law (1) 1, 4.

291 Tomuschat (n 286) 24ff; contra: Peters (n 290) 9.

292 Tomuschat ibid.

293 ibid 25.

a concrete international dispute with regard to the cyber realm, on whichever aspect and of whatever intensity or possible consequences, the respective States have a legal obligation to attempt to seek a peaceful solution, but nothing more. In this sense, the obligation of peaceful settlement of disputes is a variation of the duty to cooperation. Additionally, if the dispute evolved on the grounds of unlawful behaviour of a State, the State(s) affected could have the possibility to recourse to retorsions (unfriendly acts) or counter-measures.[294]

3.3 Cooperation and Solidarity

The general duty of cooperation is to be distinguished from the 'law of coexistence' and from the political concept of 'peaceful co-existence'. The former is a legal principle deriving from the beginnings of modern international law (strongly focusing sovereignty of States), which forms the basis of the contemporary duty to cooperation.[295] The latter is a political doctrine, pursued by the Soviet Union and, with some differences, also by the Chinese foreign policy until the end of the Cold War (still endorsed in the *Constitution of the People's Republic of China*).[296]

The duty of States of cooperation has a normative character whenever it is endorsed in international treaties establishing and governing international organisations.[297] The existence of a *general* duty to cooperate and its legal character is disputed among scholars.[298] However, there are convincing indications for the normative character of a *general* duty to cooperate, when considering the interdependence of States in times of globalisation, the enormous number of intergovernmental organisations (approximately 7,000), the myriad of international treaty obligations governing almost all aspects of international relations (over 50,000 treaties are registered at the UN), and the endorsement of the duty of cooperation in the almost universal UN Charter. This finding is supported by the emergence of an intensified form of cooperation through 'transgovernmental networks', i.e., direct interaction of specialised domestic officials in informal or formal modes, which is conditioned by the 'information age' and augmenting the traditional inter-State cooperation.[299]

---

294 cf Michael N Schmitt, 'Cyber Activities and the Law of Countermeasures' in this volume.

295 Rüdiger Wolfrum, 'Co-operation, International Law of' in MPEPIL (n 2) MN 1; cf Fassbender (n 72) 3-14.

296 Carlo Panara, 'Peaceful Coexistence' in MPEPIL (n 2) MN 1ff and 29. The doctrine focuses the importance of a peaceful cohabitation, including even forms of cooperation, between 'imperialist' and socialist States that would though be not equivalent with 'peace'. See ibid 38.

297 ibid 5.

298 See for arguments pro and con: Wolfrum (n 295) 13-24; Jost Delbrück, 'The International Obligation to Cooperate – An Empty Shell or a Hard Law Principle of International Law? – A Critical Look at a Much Debated Paradigm of Modern International Law' in Holger P Hestermeyer et al (eds), *Coexistence, Cooperation and Solidarity. Liber Amicorum Rüdiger Wolfrum* (vol 1, Brill 2011) 3, 3-16.

299 Kal Raustiala, 'The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law' (2002) 43 Virginia Journal of International Law (1) 1, 3ff and 10ff.

The UN Charter sets as one of the purposes of the organisation (and indirectly as an obligation of its Member States) 'to take effective collective measures' to maintain international peace and security (Article 1(1)) and '[t]o achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character [...]'(Article 1(3)). The *Friendly Relations Declaration* emphasises the development of cooperation among States as 'of the greatest importance for the maintenance of international peace and security' (preamble, para. 5). Principle 4 of the declaration (*The duty of States to co-operate with one another in accordance with the Charter*) states:

> […] States shall co-operate with other States in the maintenance of international peace and security […]. States shall conduct their international relations in the economic, social, cultural, technical and trade fields […]. States should co-operate […] in the field of science and technology […].

Thus, given the universality of the UN and the importance of the Declaration (section 2.1), nearly all States have a conventional obligation to cooperate, also in the realm of cyberspace, as far as it supports the maintenance of international peace and security.

Furthermore, a legal obligation of States to cooperate in the arena of cyber security can be derived from the global character of cyberspace. A legal obligation to cooperate was created by international treaties governing common spaces, as in Articles II and III of *The Antarctic Treaty* of 1959, Articles III and IX-XI of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* of 1967, and Part XI of the *United Nations Convention on the Law of the Sea* of 1982. The obligation to cooperate is likewise endorsed in the myriad of international agreements governing environmental protection.[300] As described in more detail above (section 3.1.4), general principles of international law can, *inter alia,* be identified by deduction from specific legal regimes or treaty regimes (these governing globally shared resources and common spaces) and applied to the internet (as another globally shared resource) and to cyberspace (as another common space).

The term 'cooperation' is not defined by an international treaty or in another multilateral document. However, based on an analysis of the *Friendly Relations Declaration*, cooperation can be perceived as the voluntary and proactive joint action of two or more States which serves a specific objective.[301] Consequently, the duty to cooperate can be described as 'the obligation to enter into such co-ordinated action as to achieve a specific goal',[302] which can be effectively undertaken by the States working together or when the interests of the international community require a joint action.[303]

300 Wolfrum (n 295) 31.

301 ibid 2; Peters (n 290) 2.

302 ibid; Wolfrum (n 295) 31.

303 ibid.

Although the notion of 'cooperation' remains vague, the concept of solidarity indicates that cooperation in the cyber realm should show a heightened intensity. The concept of solidarity, to which some scholars[304] attribute emerging normativity (because of references in UNGA resolutions and endorsement as a legal obligation in several international treaties),[305] supports the interpretation of international law.[306] Solidarity can be understood as an intensified form of cooperation for fostering common interests and shared values.[307] Especially, the concept is underlying, *inter alia,* the legal regimes governing the globally shared resource of natural environment and the common space of the sea bed.[308] The recognition of the concept of solidarity for the arena of the internet and cyberspace is justified on the grounds that the internet presents another global resource and cyberspace another common space, which certainly is in the common interest of the international community. Additionally, it seems reasonable that an intensified interdependence in the field of global communications (leading to an international community united in solidarity)[309] would result in the need for an intensified cooperation.

Due to the global nature of the internet and cyberspace, the integrity of these 'ecosystems' and the reduction of cyber threats as relevant to national and international security can be deemed as of common interest of the international community and can only be effectively conducted by the joint efforts of all States. Therefore, States have a legal obligation to cooperate in this regard. Additionally, based on the notion of the internet as global resource and of cyberspace as common space, the cooperation should show a 'heightened' intensity. However, States have a wide discretion as to how to fulfil the legal obligation to cooperate in the cyber realm.

4. Some Thoughts *de lege ferenda* for Cyberspace

In terms of *lex ferenda*, some basic general principles of international law, as deduced from the legal regimes governing the protection of the international environment, of common spaces (sea bed, outer space, Antarctica), or the protection from globally spreading (health) infections, could be identified and applied to the internet as a globally

304 Holger P Hestermeyer, 'Reality or Aspiration? – Solidarity in International Environmental and World Trade Law' in idem (n 298) 45, 48ff; Abdul G Koroma, 'Solidarity: Evidence of an Emerging International Legal Principle' in Hestermeyer (n 298) 103, 103-130; R St John McDonald, 'Solidarity in the Practice and Discourse of Public International Law' in (1996) 8 Pace International Law Review 259, 301.

305 eg Article 3(b) of the *United Nations Convention to Combat Desertification in Those Countries Experiencing Serious Drought and/or Desertification, Particularly in Africa* of 17 June 1994, Article 3(a) of *The Constitutive Act of the African Union* of 11 July 2000 (before: Article II(1)(a) of the OAU Charter of 25 May 1963); UN *Millennium Declaration* (n 73) 6; for further references see Hestermeyer (n 304) 50.

306 Danio Campanelli, 'Solidarity, Principle of' in MPEPIL (n 2) MN 21; Hestermeyer (n 304) 48ff.

307 Wolfrum (n 295) 3.

308 Campanelli (n 306) 6; McDonald (n 304) 262 and 282-290.

309 cf Ahmed Mahiou, 'Interdependence' in MPEPIL (n 2) MN 17.

shared resource or to cyberspace as a common space (see section 3.1.4 on the juridical technique). The following deliberations *de lege ferenda* will consider, however, only the very basic principles underlying the specific regimes, as postulating utopian ideas as general principles of international law would certainly harm[310] the normativity of law.

It should be mentioned that all principles as subsequently described can also be indirectly deduced from the principles of equal sovereignty of States and the duty of cooperation. Additionally, it can be asserted that the *de lege ferenda* application of the principle of sustainable development and equitable utilisation of global resources (4.1), of common heritage or concern of humankind (4.2), and of the protection against globally spreading (health) infections (4.3) to the internet or to cyberspace would certainly support the legal obligation of States to the maintenance of international peace and security and, in a broader sense, of removal of various threats to peace and security.

4.1 Sustainable Development and Equitable Utilisation of Shared Resources

The principle of sustainable development was first mentioned within the UN in the 1970s, pointing out the linkage of long-term development (in particular, of the so-called 'Third World') and environmental protection, and has since then been referred to in a multitude of legal and political documents.[311] The concept is based on the notion that development which meets the needs of the present generation shall not compromise the abilities of future generations, and that the use of natural resources shall be conducted in accordance with ecological, economic and social considerations.[312] It is disputed whether sustainable development is a political ideal or whether it can be deemed as a rule of international customary law.[313] One of the sub-categories of the concept, the rule of sustainable use (with regard to natural resources), is, however, widely attested to have the character of a norm of international customary law, due to its endorsement in a large number of international environmental protection agreements.[314] Additionally, the principle of equitable utilisation of shared resources (developed in the context of international water resources and the continental shelf) is acknowledged as a general principle of international law, is endorsed in various international agreements, UNGA resolutions and political declarations, and is confirmed by international jurisprudence.[315]

310 cf von Bogdandy (n 4) 1913.

311 cf Ulrich Beyerlin, 'Sustainable Development' in MPEPIL (n 2) MN 1ff.

312 ibid 1; Wolfrum, 'General International Law' (n 2) 50.

313 cf Beyerlin (n 311) 15ff (with further references).

314 ibid 20; Lilian del Castillio-Laborde, 'Equitable Utilisation of Shared Resources' in MPEPIL (n 2) MN 2-6 (with further references); Sands (n 228) 252ff, 257ff (with further references).

315 cf del Castillio-Laborde (n 314) 8ff (with further references) and 27. See also *Report of the Expert Group Meeting on Identification of Principles of International Law for Sustainable Development* (Geneva, Switzerland, 26-28 September 1995, Prepared by the Division for Sustainable Development for the UN Commission on Sustainable Development) para 38 and 48-50.

Therefore, the rule of sustainable and equitable use of resources can be deemed a general principle of international environmental law, and can be applied (see section 3.1.4 for juridical technique) to the internet as another globally shared resource, establishing a legal obligation of States to cooperate in its sustainable and equitable usage.[316] This assumed, the principle shows relevance to the internet in a twofold manner:

(1) At the first sight, the internet could be seen as not exploitable in terms of usage. This is not true, as the internet is conditioned by the possibility of individual connectivity to the web, which requires an IP address[317]. The Internet Protocol version 4 (IPv4), currently used in most parts of the globe, provides only approximately four billion IP addresses, which was deemed sufficient in the pioneer days of the internet but have been officially exhausted since February 2011.[318] Nowadays, the Internet Protocol version 6 (IPv6) can provide approximately 340 sextillion IP addresses, which is presently considered as more than sufficient for the world population of about seven billion (enough for many trillions of IP addresses to be assigned to every human being).[319] However, IPv6 is not compatible with IPv4 and is implemented only in some parts of the world.[320] This means that, despite the technological advance, IPv6 communication needs very often to be 'channelled' through the existing and limited IPv4 communication lines. Once implemented globally, IPv6 will, *de facto,* eliminate the notion of 'exploitation' of the global resource and mitigate the challenge of equitable distribution of access to, and thus use of, the internet. However, the IPv6 address range, although extremely large, it is not indefinite. Future developments can prove the number of IP addresses as not 'enough for everybody', e.g., when considering the enormous need for IP addresses by future manufacturing by 'smart factories', combining globally distributed production processes via wireless local area networks (WLANs) and thus requiring masses of IP addresses. In this context, a 'lesson identified' from the past should not be ignored: Bill Gates is said to have stated in 1981 that '640K ought to be enough for anybody',[321] a prediction undeniably proven wrong even with regard to the private use of computers. Therefore, the 'exploitation of the internet' is, in theory, conceivable. The consequence of this presupposition is a reasonable, equitable use of IP addresses in terms of an internationalised, just

316 On obligations cf del Castillio-Laborde (n 314) 15, 25.

317 An IP address (Internet Protocol number) is a 12 digit number identifying a computer or other network device during an internet session. An IP data package is the basic element of data transmission via the internet. It comprises a header (information on the source, destination, status and fragmentation of the transmitted data) and a payload (transmitted data).

318 Internet Society, IPv6 <http://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6>; IANA, Number Resources <http://www.iana.org/numbers>.

319 ibid. For explanation of the numbers of IP addresses see <http://www.brucebnews.com/2010/10/ipv6-and-really-large-numbers/>.

320 cf Internet Society, IPv6 (n 318).

321 <http://en.wikiquote.org/wiki/Talk:Bill_Gates>.

and fair regime for their worldwide distribution (conducted at the present by ICANN[322]).

(2) The legal obligation of 'sustainable use' of the internet, recognising the needs and interests of future generations, could also result in an obligation of States to undertake all necessary means of a strategic, political, legal, administrative, organisational and technical nature at an international (cooperatively) and national (individually) level in order to preserve the internet (and thus also cyberspace) for future generations as an available and reliable platform of political, economic, social and cultural interaction for all users. This connotes the restraint from any governmental action which could hamper the availability and reliability of the internet, and the proactive countering of cyber threats; even those irrelevant to national and international security.

4.2 Common Heritage or Concern of Humankind

The principle of common heritage of humankind is underlying and governing the treaty-based regimes of certain common spaces (*res communis omnium*), namely:

- the seabed (Part XI of the UN *Convention on the Law of the Sea* of 1982),
- outer space (Article 1 of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* of 1967, Article 11(1) of the *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* of 1979), and
- Antarctica (para. 8 of the preamble of the *Protocol on Environmental Protection to the Antarctic Treaty* of 1991).

Although the application of the principle varies in the different legal regimes, and is probably not intended to be fully defined, some common features can be identified, such as:[323]

- exclusion of claims of sovereignty (non-appropriation; open to use by all),
- international management (by the mankind as a whole),

322 See supra n 175. Since February 2005, ICANN delegates the assignment of IP addresses to individual users of IP address ranges to ISPs to five *Regional Internet Registries* (RIR), ie, regional organisations assigning IP addresses. Currently, these are: AfriNIC (Africa), APNIC (Asia and Pacific), ARIN (mainly North America), LACNIC (Latin America and parts of the Caribbean Region) and RIPE NCC (Europe, Middle East and Central Asia). The RIRs assign the IP addresses to local organisations, mainly to ISPs (eg, yahoo, gmail, etc). Usually, an internet user receives from the pool of IP addresses at the disposal of an ISP a specific (dynamic) IP address for the particular internet session only. After the particular internet session the dynamic IP address is assigned to another user and client of the respective ISP.

323 Rüdiger Wolfrum, 'Common Heritage of Mankind' in MPEPIL (n 2) MN 11-24.

- obligation to:
  - international cooperation in use and exploration (regulated, equal distribution to benefit of all humankind with regard to utilisation and exploration),
  - respect for interests of future generations in making use,
  - usage for peaceful purposes only.

The principle of common heritage of humankind is also applied to other common spaces than the above-mentioned, namely to the high seas, the atmosphere, and to the natural environment as such (using the term of common 'concern' of humankind with regard to the latter).[324] It is also asserted that the principle could be applied outside of common spaces, namely to living resources.[325] Thus, although the principle of common heritage (or concern) of humankind was not meant to constitute an independent principle, its application outside the respective, above-mentioned treaty regimes, i.e., to cyberspace, seems to be, in theory, adequate. This is supported by the assertion that the principle has obtained the character of international customary law with regard to the use of common spaces (resulting in obligations to international cooperation, use for peaceful purposes, equal distribution of usage and exploration, and respect for future generations).[326]

Although cyberspace can surely be deemed a common space or 'global common' in general terms, it is questionable whether it has developed[327] to a *res communis omnium* in the legal sense. Cyberspace, understood as a universal, non-physical, conceptual space, including, *inter alia,* information and a 'global public memory' (see definition in section 1) involves the notion of the internet. The physical and technical components of cyberspace, i.e., the internet, are subject to territorial sovereignty of diverse States, although forming in its assemblage a global resource. Thus, only within the notion of the internet as a whole, i.e., as a global resource, the exclusion of claims of sovereignty (and appropriation by governmental and/or private owners of technical components of the internet) can be affirmed and the principle of common heritage or concern of humankind could be applied to cyberspace.[328] However, the global internet, although managed mainly by the (privately-owned or governmental) ISPs, can be deemed as 'governed' by ICANN (based on a multitude of agreements with a myriad of stakeholders), an NGO of an internationalised character, however, acting on behalf of and reporting to the US government (see above, section 3.1). Therefore, it can be either accepted or doubted whether the aspect of an 'international management' of the internet is established.

If the internet, and thus cyberspace, was considered a common heritage or concern of humankind, States would have the obligation to, *inter alia,* use it for peaceful purposes

324 ibid 9; Crawford (n 11) 333.

325 Wolfrum, 'General International Law' (n 2) 61.

326 idem (n 323) 25.

327 Affirming cyberspace as *res communis omnium*: Heintschel von Heinegg (n 200) 9.

328 ibid.

only. This corresponds with the general principle of international law to refrain from the threat of or the use of force in international relations, and would still allow the military use of cyberspace for, e.g., exercises, self-defence, or measures undertaken according to Chapter VI and VII of the UN Charter. Although some States refer to cyberspace as a 'global common',[329] the official diplomatic language partly avoids terminology which could indicate the development of the internet or of cyberspace into a common heritage or concern of humankind (e.g., Germany speaks of a 'public good'[330]). Thus, tendencies for respective developments are currently not detectable.

4.3 Protection against Globally Spreading Infections: The World Health Regime

International cooperation in the field of transboundary spreading of health infections had already begun in the 19th century.[331] It was motivated by technological advances of communication and transportation, which led to intensified economic exchanges and international relations.[332] The World Health Organization (WHO), established in 1948, is providing leadership on global health matters, setting norms and standards, articulating evidence-based policy options, providing technical support to countries as well as monitoring and assessing health trends.[333] According to Article 21 of the *Constitution of the World Health Organization* of 1946 (WHO Constitution), the Health Assembly (pursuant to Article 10 composed of delegates representing all Member States) has the authority to adopt regulations on:

(a) quarantine requirements and other procedures designed to prevent the international spread of disease,

(b) nomenclatures with respect to diseases,

(c) standards on safety and other areas,

(d) standards on purity of products moving in international commerce, and

(e) advertising and labelling of products moving in international commerce.

According to Article 22 of the WHO Constitution, the regulations come into force by use of a silent-procedure. Such International Health Regulations (IHR) entered into force in 2007, and are legally binding on 194 countries across the globe, including all Member States of the WHO.[334] They define, *inter alia,* the obligations of States to

329 eg Japan, Ministry of Defence, *Toward Stable and Effective Use of Cyberspace* (September 2012) 2; US Department of Defence, *The Strategy for Homeland Defence and Civil Support* (2005) 12.

330 Permanent Mission of the Federal Republic of Germany to the United Nations, New York, Note Verbale/Note No 516/2012 (November 2012) <http://www.un.org/disarmament/topics/informationsecurity/docs/Germany_Verbal_Note_516_UNODA.pdf>.

331 Yves Beigbeder, 'World Health Organization (WHO)' in MPEPIL (n 2) MN 2.

332 ibid.

333 WHO, About WHO <http://www.who.int/about/en/>.

334 idem, 'What are the International Health Regulations?' <http://www.who.int/features/qa/39/en/index.html>.

report public health events and require States to strengthen their existing capacities for public health surveillance and response.[335] Furthermore, pursuant to Article 28(i) of the WHO Constitution, the WHO Board (consisting of 34 persons designated by the Health Assembly, Article 24) has the authority 'to take emergency measures […] to deal with events requiring immediate action.'

Based on the truly universal normativity of the IHR, a general principle of international law in the form of an obligation of intense cooperation between States for the prevention and combat of infections (or diseases) can be derived from that legal regime (including obligations to inform, notify, and consult). However, the application (see section 3.1.4 for the juridical technique) of the principles underlying the IHR to the situation of transboundary spreading of computer viruses, worms and other malicious software does not seem justified, as the impact of malicious software on world populations is very different in its intensity and significance from the impact of globally spreading health infections and diseases. The massive negative impact of cyber manipulations on economies, which cannot be denied, does not vindicate the application of the principles of health regulations to the internet or to cyberspace.

However, empowering an international entity with authorities comparable to those which the WHO Health Assembly and Board have (see above) should be considered. As the impact of cyber threats on national and international security will surely intensify in the future due to technological advances and a growing dependence on the global net, such an international entity could adopt regulations similar to IHR, regarding:

- strengthening national capacities for cyber hygiene surveillance and response,
- reporting of cyber security incidents,
- quarantine requirements for networks,
- nomenclatures (or catalogues) of malicious software,
- standards of cyber security,
- standards of purity of software,
- advertising and labelling of software, and
- taking emergency measures in cases which require immediate action.

5. Summary and Conclusions

General principles of international law can be derived, *inter alia,* from general considerations, legal logic, legal relations in general, international relations, or from a particular treaty regime. Hitherto, neither international courts nor scholars have developed a methodology for identifying the principles. However, with regard to general principles of international law as pertaining to international peace and security,

[335] ibid.

international courts and academia acknowledge the existence of several principles based on sovereign equality of States, the duty to the maintenance of international peace and security, and the duty to international cooperation in solving international problems. These principles (and their sub-principles or corollary principles) are endorsed in Article 1 and 2 of the UN Charter and confirmed by the UNGA *Friendly Relations Declaration*, as well as, for example, the *Helsinki Declaration*. General principles of international law may serve different purposes, of which the most significant is the function as a basis for the progressive development of international law (either by filling a legal *lacuna* or by progressive interpretation of existing international norms), responding to rising extra-positive needs of the international society, such as fast growing technical advances, e.g., the 'emergence' of cyberspace as a common space for inter-State relations.

Sovereignty, although strongly affected by interdependence, globalisation, and the emergence of international organisations, among others (which is especially true for cyberspace, introducing vertical and diagonal relations between all stakeholders), is the core of the notion of statehood and an axiomatic principle upon which international law is based. The following obligations and rights of States can be deemed as deriving from the equal sovereignty of States, and from principles respectively de-conflicting the competing sovereign rights within the international community:

- Based on legal logic, no State can claim sovereignty over the global resource that is the internet or the common space of cyberspace. This finding is supported *de lege ferenda* by the principle of common concern of humankind.
- Based on the principle of territorial sovereignty, a State may regulate, within the boundaries of its own territory, internet activities (also with regard to contents) of its own or foreign nationals, if these are conducted on its territory or show effects on its own territory. States need especially to consider human rights law with regard to the right to access to the internet.
- Based on the principle of territorial sovereignty, the duty not to harm other States' rights, the principle of good neighbourliness and the *sic utere tuo* principle, a State is forbidden to cause physical effects to technical components of the internet located on the territory of another State or to cause other effects relevant to the national security of the affected State.
- Based on the preventive principle deriving from the 'no-harm rule', the principle of good neighbourliness and the *sic utere tuo* principle, States have the obligation to prevent malicious cyber activities which could harm the rights of other States, and thus to:
    - ensure that national ISPs install network sensors collecting information on the 'net flow', i.e., amount of routed data and their destination (allowing to detect, e.g., 'DDoS attacks'),

  - ensure that national tier 1 ISPs install intrusion detection/prevention systems at their 'gates' of international data transmission, conducting deep package filtering (allowing recognition of malicious software),
  - establish a respective obligatory reporting system of ISPs to a governmental entity (e.g., a national or governmental CERT),
  - establish a respective framework of strategic, political, legal, administrative, organisational and technical nature allowing to conduct the above-mentioned measures as well as to ensure effective management of prevention of malicious cyber activities potentially harming other States' rights (including risk assessment, as well as notification and information of and consultation with other States),
  - establish investigative cyber capabilities (allowing the identification of the source of the malicious cyber activities),
  - establish an organisational and legal framework allowing the prevention or discontinuation of concrete malicious cyber activities originating on the State's territory and potentially harming the rights of other States.
- Based on the precautionary principle (deduced from the legal regimes governing global resources and common spaces) or on a 'due diligence' principle (derived from the 'no-harm' rule), as well as on the principle of good neighbourliness and the *sic utere tuo* principle, States are obliged to establish a national cyber security framework. This finding is supported *de lege ferenda* by the principle of sustainable development of global resources, and by the principle of common concern of humankind.
- Based on the preventive principle deriving from the 'no-harm rule', the principle of good neighbourliness and the '*sic utere tuo*' principle, States are obliged to inform, notify, and consult other States in situations of concrete cyber incidents which are likely to cause physical damage in the territory of other States or any other effects relevant to the national security of other States.
- Based on the principle of (territorial) jurisdiction, States shall not conduct online law enforcement activities (e.g., online search) in networks located on another State's territory. However, such activities do not violate the principle of non-intervention in domestic affairs of another State, as the element of 'coercion' is not present.
- Based on the duty to cooperate and on the principle of solidarity, States are obliged to establish and maintain an intensified cooperation in the cyber realm. Due to the principle of (competing and overlapping) jurisdiction, States shall cooperate closely in law enforcement activities in cyberspace. This results in the obligation

of the establishment of the organisational, legal and (investigative) technical framework for cyber law enforcement in the realm of international cooperation.

- The principle of non-intervention in domestic affairs of another State is not violated with regard to political demands related to internet communication as such, access to internet, or cyber security, as these areas do not belong to the purely internal affairs of a State.
- Based on the duty to maintain international peace and security, States are obliged to attempt to seek a solution by peaceful means with regard to any question involving the cyber realm.
- Based on the duty to maintain international peace and security, States are obliged to refrain from the use of force by cyber means. This finding is supported *de lege ferenda* by the principle of common concern of humankind.
- *De lege ferenda*, based on the principle of equitable utilisation of shared resources and on the principle of common concern of humankind, States should establish an internationalised, just and fair regime for the worldwide distribution of IP addresses.
- *De lege ferenda*, authorities similar to those which the WHO deploys with regard to globally spreading infections (and diseases), as contained in the IHR, could be applied to cyberspace, empowering an international entity to adopt regulations on strengthening national capacities for cyber hygiene surveillance and response, cyber incident reporting, quarantine requirements for networks, nomenclatures of malicious software, standards of cyber security, standards of purity of software, advertising and labelling of software, and taking emergency measures in cases which require immediate action.

Although States in general prefer to maintain a strategic ambiguity with regard to questions related to use of force and armed attack, thus leaving the respective debate to academia, it would certainly support predictability and stability in international relations if they shared their views on aspects of the 'use of [armed] force' in cyberspace, 'armed attack' and preventive self-defence in cyberspace, non-State actors as potentially triggering the right to self-defence, the 'safe haven' theory and the 'accumulation of events' or *Nadelstichtaktik* theory with regard to malicious cyber activities. Also, States should clarify the role of the armed forces with regard to ISPs and CERTs of industry providing critical infrastructure, who will conduct concrete defensive measures on a 'bit for bit' basis in the case of an 'armed attack' targeting such infrastructures.

It should be emphasised that, despite their generality and the value-based differences present within the international community, general principles of international law are recognised as a normative source of law, either as part of international customary law or as a separate source of international law. Following a specification of their contents

by interpretation, as proposed in the present chapter, general principles of international law achieve the quality of a 'hard law' right or obligation of a State.

Importantly, due to their nature as the foundation of the international law system, it is widely recognised within scholarly writings that such general principles of international law pertaining to international peace and security, as presented above, are essential for the 'co-existence and vital co-operation of the members of the international community', and thus exist irrespective of the States' (other) practice, *opinio iuris*, consent or any other expression of will. Moreover, such basic principles enjoy a 'heightened' normativity – without introducing a formal hierarchy to the sources of international law – because of their *quasi*-constitutional role within the international law system or as peremptory norms of international custom.

This results in the utmost important finding that States cannot 'opt out' from basic general principles of international law of which an interpretation – with regard to governmental activities in cyberspace – was offered in the present chapter.

*Benedikt Pirker**

Territorial Sovereignty and Integrity and the Challenges of Cyberspace

1. Introduction

It is now widely recognised that the rules of international law also apply to cyberspace, 'to be ignored by the digitally distracted at their own peril'.[1] Much ink has been spilt on topics concerning cyber war;[2] but many questions of what rights and obligations States possess in peace-time remain to be answered.[3] This contribution aims to provide an overview of the various legal issues that arise from the concepts of territorial sovereignty and integrity of States in international law. As a number of other contributions focus in detail on elements evoked in this context, the present chapter deliberately refrains from detailed engagement with some issues, providing an overview rather than an in-depth discussion. The assessment shows that, while a number of prescriptions of international law are pertinent for territorial sovereignty and integrity in cyberspace, their exact content remains to be spelled out by future State practice and perhaps case law. The emerging dilemma can be described in the following manner: the imposition of excessive requirements on States within the realm of their own territorial sovereignty, which would require an inflated or even impossible level of supervision and regulation of cyberspace, must be avoided; at worst, such requirements could increase the potential for inter-State tensions in an area where operations are particularly difficult to identify and attribute to a particular State with sufficient clarity. However, adopting a laissez-faire approach by loosely interpreting the obligations incumbent on States could leave other States without effective legal redress under international law against impermissible interferences with their territorial sovereignty and integrity.

* The author would like to thank Astrid Epiney, Kaur Kasak, Markus Maybaum, Ziv Bohrer, Robert Mosters, Markus Kern, Thomas Burri and Katharina Ziolkowski for valuable assistance during the drafting process of this contribution.

1 MJ Glennon, 'The Road Ahead: Gaps, Leaks and Drips' (2013) 89 International Law Studies 362, 377. See more on the topic in section 2.2.

2 See e.g. on the notion of what constitutes an armed attack MC Waxman, 'Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions' (2013) 89 International Law Studies 109, 111 ff.; on the obligations of neutral States in a situation of cyber war S Kanuck, 'Sovereign Discourse on Cyber Conflict under International Law' (2009-2010) 88 Texas Law Review 1571, 1593; JE Kastenberg, 'Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law' (2009) 64 Air Force Law Review 43, 44.

3 See, for one of the very rare contributions on the issue, W Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' (2012) 4th International Conference on Cyber Conflict 7; slightly modified in W Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 International Law Studies 123.

In terms of the structure of this contribution, section 2 addresses the notion of territorial sovereignty and integrity under international law and discusses how the specificities of cyberspace can be accommodated under it. The subsequent section assesses the scope of territorial sovereignty and issues of extraterritoriality as applicable to cyberspace. The fourth section evaluates the content of territorial sovereignty and integrity based on the notion of non-intervention, assessing the duties of States with the help of concrete examples of potentially problematic cyber activities. Based on these findings on the obligations of States and potential violations of international law through cyber activities, the fifth section examines possible reactions, in particular State responsibility, countermeasures and the invocation of the defence of necessity, with all the complications caused by the technical specificities of cyberspace which, in particular, render the attribution of acts to States a complex task. A final section concludes, evaluating future steps and in particular the potential of global rules and the difficulties attached to their creation.

The aim of this contribution is to present and discuss the state of international law. A central support in this regard is the recently published *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[4] a proposed guide to the state of customary international law drafted by an expert group[5] which also contains a number of rules relevant for the topic of territorial sovereignty and integrity.

2. The Notion of Territorial Sovereignty and Integrity under International Law and the Applicability of International Law to Cyberspace

Definitions of territorial sovereignty and integrity and what functions they serve under general international law form a necessary starting point for the discussion, together with a confirmation that – despite some earlier controversies on the issue – the rules of international law apply to cyberspace.

2.1 Territorial Sovereignty and Integrity under International Law

Territorial sovereignty is an essential aspect of sovereignty as a crucial capacity of the State, sovereignty with its rights and duties being a pillar of international law and 'founded upon the fact of territory'.[6] For Arbitrator Huber in the famous *Island of*

4 MN Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, Cambridge 2013).

5 On the drafting method of the Manual, see MN Schmitt, 'Introduction' in MN Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, Cambridge 2013), 6. Some early sceptics have pointed out that there may be an overtly close connection of the expert group to the military and a potential resulting bias in the substance of the Manual. O Diggelmann, 'Militärische Gewalt bei Cyberattacken', *Neue Zürcher Zeitung* (30 May 2013).

6 MN Shaw, *International Law* (6 edn Cambridge University Press, Cambridge 2008), 487.

Palmas case, sovereignty mostly signified '[i]ndependence in regard to a portion of the globe' as 'the right to exercise therein, to the exclusion of any other State, the functions of a State'.[7] Territorial sovereignty is thus a State's right, but it entails at the same time a duty 'to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war'.[8]

Based on these findings, the notion of sovereignty can to some extent be distinguished from that of integrity. Sovereignty – in the sense of territorial sovereignty – refers to a State's privilege of exclusive exercise of its powers on its territory. Integrity focuses on the State's right to be free of interference or, seen from another State's perspective, the duty to avoid interference with the territorial integrity of said State. Both are inextricably linked or 'correlated principles'[9] and it is in this sense that these terms will be used in this contribution.

As regards sovereignty, the International Court of Justice (ICJ) has underlined that 'respect for territorial sovereignty is an essential foundation of international relations'.[10] Moreover, the *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, adopted in 1970 by the United Nations General Assembly, confirmed that '[n] o state or group of states has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other state'.[11] Territorial sovereignty also includes political independence of a State, that is, full control of the said State over its organs.[12] This independence should enable a State to freely pursue the path to the economic, social and cultural development of its choice without being coerced in any way.[13] Coercion is a crucial term in this regard, as the subsequent discussion of territorial integrity will show.

Territorial sovereignty generally extends over the territory of a State and protects it from undue interference by any other State. Cyber infrastructure located within the territory of a State is thus protected through the State's territorial sovereignty[14] and at the same time subject to the State's territorial jurisdiction: the State can thus 'regulate, restrict or prohibit' access to cyber infrastructure both from within and

7 *Island of Palmas Case (Netherlands v. USA)* 4 April 1928, Reports of International Arbitral Awards, Volume II pp 829-871, 838.

8 Ibid., 839.

9 S Besson, 'Sovereignty' in R Wolfrum (ed) *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, Oxford 2012), 376 para 70.

10 *The Corfu Channel Case (United Kingdom v. Albania)* ICJ Reports 1949, 4, 35.

11 U.N. Doc. A/8028 (24 October 1970), 121 ff.

12 SKN Blay, 'Territorial Integrity and Political Independence' in R Wolfrum (ed) *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, Oxford 2012), 861 para 9.

13 Ibid., 862 para 18 with reference to the Friendly Relations Declaration.

14 *Tallinn Manual*,16 para 5 (Rule 1 Sovereignty).

outside its territory.[15] Coastal States also possess territorial sovereignty over the seabed beneath the territorial sea and therefore potentially over submarine cables.[16] Territorial sovereignty can, however, be limited by international law. Typical examples include the protection of diplomatic premises and personnel, and restrictions on a State's power to regulate access to the internet based on human rights obligations[17] or international telecommunication law.[18]

Territorial integrity can be understood as the protective dimension of statehood in international law. Two kinds of interventions can constitute a violation of the territorial integrity of a State. First, interventions using force already fall under the prohibition of Article 2 (4) of the *Charter of the United Nations* (UN Charter); but other interference with a State's territorial integrity can also amount to a violation under international law, often derived from the principle of sovereign equality of States as enshrined in, for example, Article 2 (1) of the Charter. For this second category, the notion of coercion is the central tenet.

While coercion of a State through economic or political measures is typically not regarded as a violation of the prohibition to use force,[19] it can amount to a violation of territorial integrity if it displays sufficient intensity.[20] Another well-known example of a violation of the principle of non-intervention[21] is support granted by one State to subversive groups such as rebels who want to overthrow the government of another State.[22]

In the *Nicaragua* case, the ICJ made it clear that there is a certain threshold where mere interference turns into prohibited intervention. According to the Court, 'a prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy.'[23] For the Court, the 'element of coercion' not only 'defines', but 'forms

15 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace' 14.

16 *Tallinn Manual*, 17-18, para 11 (Rule 1 Sovereignty). For more detail on this issue, see W Heintschel von Heinegg 'Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law' in this volume.

17 See in this respect on the emerging notion of internet access rights as human rights JW Penney, 'Internet Access Rights: A Brief History and Intellectual Origins' (2011-2012) 38 William Mitchell Law Review 10.

18 *Tallinn Manual*, 17 paras 9 and 10 (Rule 1 Sovereignty).

19 See also on the UN Charter in this regard JL Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24 European Journal of International Law 129, 133.

20 J Combacau and S Sur, *Droit International Public* (Montchrestien, Paris 2012), 266.

21 For an in-depth account of the concept of non-intervention in domestic affairs, see TD Gill, 'Non-Intervention in the Cyber Context' in this volume.

22 *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)* ICJ Reports 1986, 14, para 205.

23 Ibid.

the very essence of […] prohibited intervention'.[24] The quotation also shows that, for the purposes of establishing a violation, no clear-cut distinction is drawn between the notions of sovereignty and integrity, showing again that they are inextricably linked.

With these principles applicable under territorial sovereignty and integrity in general public international law in mind, it should now be examined whether cyberspace as a space follows the same rules.

2.2 The Applicable Law for Cyberspace

In the early days of the internet, controversy emerged over the question of whether cyberspace should be covered by the usual rules of law, in particular international law, or whether a new space had emerged which would not be subject to traditional notions and rules of law.

Famously, in his '*Declaration of the Independence of Cyberspace'* Barlow argued that cyberspace should be left to its own inhabitants who would create the necessary self-regulation.[25] His main argument was that there was no single legitimate decision-maker for cyberspace in international law.[26] Others did not go as far, but still suggested that a special internet law was required to ensure sufficient space for self-regulation of actors in the new space that had emerged.[27] Such 'cyberspace autonomy'[28] was contested by those who thought that a special legal regime for cyberspace was unnecessary. Easterbrook famously claimed that establishing a specific discipline of cyber law made as little sense as to have a special 'law of the horse'.[29] As the present state of regulation of cyberspace illustrates, the conflict between 'cyber-libertarians and cyber-legal-positivists'[30] resulted in a victory of the latter, more traditional approach. This approach suggested that cyberspace should be subject to the standard rules of jurisdiction and of the national law of the competent State. The central argument for scholars like Goldsmith was that cyberspace was no special space, but had a predominant connection to the real world,

24 Ibid.

25 JP Barlow, 'A Declaration of the Independence of Cyberspace' (1996) Electronic Frontier Foundation (Feb 8, 1996), <https://projects.eff.org/~barlow/Declaration-Final.html> 1. See on the surrounding 'law and technology' debate M Birnhack, 'Reverse Engineering Informational Privacy Law' (2012) 15 Yale Journal of Law and Technology 24, 33.

26 See on Barlow's claim A Murray, 'Of Uses and Abuses of Cyberspace: Coming to Grips with the Present Dangers' in A Cassese (ed) *Realizing Utopia - The Future of International Law* (Oxford University Press, Oxford 2012), 500.

27 DR Johnson and D Post, 'Law And Borders - The Rise of Law in Cyberspace' (1995-1996) 48 Stanford Law Review 1367.

28 J Kulesza, *International Internet Law* (Routledge, London 2012), 146.

29 FH Easterbrook, 'Cyberspace and the Law of the Horse' (1996) University of Chicago Legal Forum 207. See on the context of Easterbrook's well-known pronouncement G Lastowka, 'Paving the Path of Cyberlaw' (2011) 38 William Mitchell Law Review 1, 1. See, by contrast, the reply to Easterbrook by L Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501.

30 Murray, 499.

with its equipment, with users acting in a State's territory and with the effects of cyber activities and transactions in one or more States, that could be felt and measured in other States.[31]

Consequently, cyberspace did not emerge as a new dimension, but has continuously been subject to State practice acting according to the traditional rules of international law, in particular as regards the exercise of jurisdiction.[32] In more recent scholarship, general questions of the legitimacy of jurisdiction over cyberspace have thus been qualified as 'first generation issues', while attention has in the meantime moved towards more relevant 'second generation issues' such as the actual enforcement of judgments in cyberspace-related cases and the concrete application of conflict of laws rules.[33]

3. The Scope of Territorial Sovereignty in Cyberspace

Cyberspace is thus a space to which the territoriality vocabulary of international law applies in principle. Consequently, this section first examines some existing proposals to give cyberspace a special status under international law. Given the present state of international law, no such special status is recognised. States thus regulate cyberspace in relation to their territory and in accordance with the rules on the exercise of jurisdiction, which are generally accepted in international law and will be examined subsequently.

3.1 The Territorial Status of Cyberspace

Cyberspace's special nature has led scholars to suggest that it should enjoy a special legal status. Cyberspace is ubiquitous and cannot be entirely appropriated by one State. Analogies have been drawn to spaces with a particular legal regime in international law such as outer space or the high seas.[34] Proposals to view cyberspace as a 'global common',[35] however, seem to have failed to gather widespread consent to date. As a starting point, there certainly exists a real-world technical infrastructure on which cyberspace is based, which is owned by governments and corporations. The mere fact of the connection of this infrastructure to the global network of cyberspace cannot simply be equated with a waiver of territorial sovereignty.[36]

31 JL Goldsmith, 'Against Cyberanarchy' (1998) 65 University of Chicago Law Review 1199.

32 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace' 8.

33 M Reimann, 'The Yahoo Case and Conflicts of Law in the Cyberage' in C Ku and PF Diehl (eds), *International Law - Classic and Contemporary Readings* (Lynne Rienner, London 2009), 459.

34 PW Franzese, 'Sovereignty in Cyberspace: Can It Exist?' (2009) 64 Air Force Law Review 1, 18 ff.; Kulesza, 146 ff.

35 See also on this issue K Ziolkowski 'General Principles of International Law as Applicable in Cyberspace' in this volume.

36 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace' 9-10.

Furthermore, a number of reasons explain why the 'global commons' approach fits rather poorly in the case of cyberspace. First, there is no real 'tragedy of the commons'.[37] This would only be the case in a situation where the indiscriminate use of a common resource by all would inevitably diminish or degrade the resource in the long term: think, for example, of the regulatory regime on fisheries. Second, a global commons regime would require common rules, but identification and attribution problems make it difficult to enforce such rules.[38] Lastly, from a political economy perspective, the infrastructure of cyberspace remains subject to private property rights, which would make expropriation at a large scale inevitable for a global commons regime; also, as to regulating access, the identification and thus exclusion of illegitimate users is hardly technically feasible.[39]

Some have suggested that, instead of granting global commons status to cyberspace, at least certain 'critical internet resources' ought to be regulated under international law as 'Common Heritage of Mankind'.[40] This status would grant freedom of access and exploration without discrimination for all States to a certain territory.[41] The present condition of cyberspace regulation, however, remains much less advanced. The regulatory architecture of the internet essentially remains limited: As one central function, the attribution of domain names was entrusted to a non-profit corporation, the Internet Corporation for Assigned Names and Numbers (ICANN), located in the United States of America, being supervised by the United States Department of Commerce.[42] Since 2009, the Affirmation of Commitments reformed the operation of ICANN, giving more room for stakeholder representation for both civil society and national governments and increasing the transparency of decision-making.[43]

Still, as a matter of principle, cyberspace remains a space subject to the normal rules of jurisdiction of international law. To speak of a 'virtual jurisdiction' is thus just as much a misnomer as to expect treatment of cyberspace as a 'global common'.[44] A trusteeship could be a more suitable solution in the future, but such global rules have

37 See generally on the notion G Hardin, 'The Tragedy of the Commons' (1968) 162 Science 1243.

38 See more on this topic in section 5.1.

39 This overview of reasons is based on Kanuck, 1578 ff.

40 A Segura-Serrano, 'Internet Regulation: A Hard-Law Proposal' (2006) 10 Jean Monnet Working Paper 1, 48.

41 See e.g. Article 1 of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, 27 January 1967.

42 See, on the old status of ICANN, B Carotti and L Casini, 'A Hybrid Public-Private Regime: The Internet Corporation for Assigned Names and Numbers (ICANN) and the Governance of the Internet' in S Cassese and others (eds), *Global Administrative Law - Cases, Materials, Issues* (2 edn, IRPA-IILJ, Rome-New York 2008), 29 ff.

43 See, for detail on the reform, Kulesza, 132-133. See also, more broadly on ICANN's regulatory functions and dispute resolution system, F Casarosa, 'Transnational Private Regulation of the Internet: Different Models of Enforcement', in F Cafaggi (ed), *Enforcement of Transnational Regulation – Ensuring Compliance in a Global World* (Edward Elgar, Cheltenham 2012), 279 ff.

44 Kanuck, 1573.

yet to see the light of day. Under such a legal regime, States have to bear the costs and carry the responsibility for a specified area; at the same time they have to grant equal access and opportunity to everyone.[45] Under extant international law, however, activities in cyberspace fall under the normal rules of international law on the exercise of jurisdiction.

3.2 The Exercise of Jurisdiction and Extraterritoriality in Cyberspace

Jurisdiction – 'the power of the state under international law to regulate or otherwise impact upon people, property and circumstances'– is a 'vital and indeed central feature of State sovereignty'.[46] A State's power reaches beyond its territory and, for example, the cyber infrastructure located within it: States can use their legislative, executive and judicial jurisdiction in relation to events and persons on their territory, and also in relation to events and persons in the territory of other States, but will face the problem that no enforcement is possible in the territory of another State; furthermore, some exercises of jurisdiction may amount to a violation of the sovereignty and independence of another State.[47]

Under general international law, a number of connecting factors are accepted as the basis for States to exercise their jurisdiction. As a matter of principle, States go further in claiming jurisdiction in civil law matters when compared to criminal law, as the resulting reaction by other States tends to be 'much more muted' in the case of the former as compared to the latter.[48] Despite such finesse, the generally applicable factors can be outlined as follows.

Based on the territoriality principle, States are able to legislate with regard to activities and to prosecute offences committed on their territory. This linking factor is perhaps the least contested of all in international law.[49] The nationality principle allows a State to regulate persons based on the genuine legal link and reciprocal rights and duties existing between a State and its nationals.[50] States thus claim jurisdiction over crimes committed by their nationals, although some tend to do so only for very serious offences.[51] Using the passive personality principle, States regulate cases where one of their nationals falls victim to a criminal offence, irrespective of the location or nationality of the perpetrator.

45 Ibid., 1579-1580, refers to the example of the legal regime covering the Svalbard archipelago which imposes such obligations upon Norway and restricts the country's sovereignty for this purpose.

46 Shaw, 645.

47 Ibid., 650, gives the general international law example of a French law ordering all French citizens living abroad to drive exclusively French cars.

48 Shaw, 651.

49 Combacau and Sur, 351-352.

50 See, on that link, *Nottebohm Case (Liechtenstein v. Guatemala)* ICJ Reports 1955, 4, 23.

51 Shaw, 663.

While initially contested, the principle 'today meets with relatively little opposition'.[52] The protective principle enables a State to exercise jurisdiction over a situation in which its security interests are at stake. It has also been codified in a number of international treaties.[53] The universality principle provides that States can claim jurisdiction to try offences of a particularly grave nature, such as piracy or certain war crimes.[54] Lastly, the effects principle is perhaps still the most disputed link for establishing jurisdiction. Based on this principle, a State may claim jurisdiction if a certain act has sufficient effect on its territory, although the nature and gravity of the effects necessary for this purpose is hotly debated.[55]

These various principles can be used by States to found their jurisdiction over persons and events. Since they may apply simultaneously and – as is particularly visible in the case of the effects principle – their exact content may be subject to varying interpretations, overlaps are possible and may also lead to conflicting exercises of jurisdiction. As these rules also apply to cyberspace, the same problems can emerge there.[56]

A good example is the *Yahoo!* case[57] in which French NGOs sued Yahoo! for making an online auction of Nazi paraphernalia on its website accessible to French internet users. Selling such objects is an offence under French law. The French court issued several interim orders requiring Yahoo! to make such auctions inaccessible to French internet users. Yahoo! sought a declaratory judgment from United States courts that enforcing the French court orders would violate its *First Amendment* rights to free speech.[58] The competent district court upheld Yahoo!'s claim. There also emerged some disagreement between courts on whether personal jurisdiction could be exercised over the French NGOs. Under United States law, there is a 'minimum contacts' requirement to the forum of a dispute for a claim concerning non-residents to be brought.[59] Eventually the

52 *Arrest Warrant Case (Democratic Republic of Congo v. Belgium)* ICJ Reports 2002, 3, 76-77 para 47 (Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal).

53 See e.g. *International Convention Against the Taking of Hostages*, adopted by the General Assembly of the United Nations on 17 December 1979, Article 5 (c).

54 Shaw, 668.

55 See also *Tallinn Manual*, 20 para 6 (Rule 2 Jurisdiction). As an example, in the landmark *Wood Pulp* case, a competition law fine imposed by the European Commission on a number of non-EU companies for a price-fixing agreement was contested before the Court of Justice of the European Union. Asked whether the behaviour could be fined under EU law merely because its effects were felt within the internal market of the EU, the Court's Advocate General argued that competition law fines could be imposed merely based on the fact that acts done by foreigners had 'direct, substantial and foreseeable effect' in the EU, see Opinion of Advocate General Darmon, Joined Cases 89, 104, 114, 116, 117 and 125 to 129/85 *A. Ahlstrom Oy v. Commission* [1988] ECR 05193, para 57.

56 See also *Tallinn Manual*, 20 para 9 (Rule 2 Jurisdiction).

57 See for a concise summary of the case M Benedetti, 'Jurisdiction over Cyberspace: YAHOO! in the French and American Courts' in S Cassese and others (eds), *Global Administrative Law - Cases, Materials, Issues* (2 edn, IRPA-IILJ, Rome-New York 2008), 216-218.

58 See on the protection of free speech on the internet the landmark case *Reno v. ACLU*, 521 US 844 (1997). See also Goldsmith, 'Cyberanarchy' 1199 f.

59 See, with additional references to the case law, Kulesza, 89 ff.

Court of Appeals upheld personal jurisdiction in the case, but dismissed the action for lack of ripeness. The Supreme Court did not agree to hear the case, while Yahoo! had in the meantime complied with the French NGO's requirements without having had to pay the French fines.

The case demonstrates two things. First, overlapping jurisdictions are commonplace, but problems caused by this phenomenon can also be resolved using the usual tools. For internet service providers this means that they will sometimes need to comply with the strictest requirements of various States,[60] or ensure by technical means that their content is not accessible in jurisdictions where such content could constitute an offence. Second, conflicting standards of, for example, fundamental rights protection can become an issue, too,[61] but this does not prevent the application of the standard conflict of laws rules.[62]

Next to conflicts of jurisdiction over substantive norms, there can also emerge *de facto* safe havens in cyberspace. In the *R v Sheppard & Anor* case, a person domiciled in the United Kingdom was successfully prosecuted for posting racially inflammatory material; the material posted, however, remained accessible online as it was hosted on a Californian web server and thus protected under the *First Amendment* to the *Constitution of the United States*.[63]

These cases demonstrate the applicability of the basic rules on jurisdiction in international law to cyberspace. The territorial principle remains strong; in *R v Sheppard & Anor*, there could be no claim to have the contentious content hosted in the United States removed, but based on the nationality principle as well as on the territoriality principle, the person posting the content could be prosecuted based on his or her citizenship of and residence in the United Kingdom. *Yahoo!* can be said to some extent to be based on the protective principle, with France trying to protect its citizens from certain content considered dangerous to public order.

The universality principle plays a minor role in the cyber context. Cyber activities are able to inflict serious economic damage, but to date have not been used to commit very serious international crimes like war crimes or genocide. Similarly, the effects principle has not been relied upon extensively by States to exercise jurisdiction over cyberspace, which corresponds to the general reticence in international law to resort to the claim of effects-based jurisdiction. Nonetheless, there remains little doubt that as soon as cyber activities reach a sufficient degree of severity, both principles may be advanced by States willing to exercise jurisdiction.

60 Murray, 503.

61 Benedetti, 218-219.

62 Reimann, 459.

63 *R v Sheppard & Anor* [2010] EWCA Crim 65, discussed in Murray, 504 f.

The current approach of potentially conflicting jurisdictions and conflicts of laws can be criticised. A case for global rules of coordination could indeed be made if one observes the potential for controversy among States and claims of violation of territorial integrity and sovereignty where jurisdictional claims seem questionable. In the absence of such governing rules, the rules of international law on the exercise of jurisdiction should, however, not easily be dismissed and continue – despite their weaknesses – to form a useful benchmark against which States can evaluate their regulatory approach to cyberspace activities.

4. The Content of Territorial Sovereignty and Integrity and the Specificities of Cyberspace

This contribution has found that territorial sovereignty is not to be conceptualised under international law in a fundamentally different way for cyberspace than for real-world territories. Consequently, the content of territorial sovereignty and integrity and the question of what constitutes a violation of territorial sovereignty and integrity should be examined. The rules and concepts applicable under international law do not change, but the specificities of cyberspace and cyberspace activities render them somewhat more challenging to apply. First, lower-level violations of territorial integrity must be distinguished from violations of the prohibition to use force; then the duties incumbent upon States based on territorial sovereignty and integrity should be examined, which includes a discussion of some typical, potentially problematic cyberspace activities.

4.1 Distinguishing Lower-Level Violations of Territorial Integrity from Prohibited Use of Force

As discussed earlier, the use of military means to intervene in another State typically falls foul of the prohibition to use force. Action below this threshold, for example coercion by economic or political means, may constitute a case of prohibited intervention into the territorial sovereignty of the victim State. The central problem is the continuing debate over what actually constitutes the use of military force in the cyberspace realm.

A number of theoretical approaches have attempted to provide a definition. Sharp draws an analogy with non-military physical violence which triggers a right to self-defence under general international law where the results are equivalent to those of an armed attack.[64] Cyber attacks would amount to a prohibited use of force, in his view, if they intentionally caused destructive effects on the territory of another State or, where only economic damage is caused, if they reached a level of intensity which threatened the sovereignty and territorial integrity of another State.[65] Heintschel von Heinegg argues

64 WG Sharp, *Cyberspace and the Use of Force* (Aegis Research Corporation, Falls Church 1999), 101.

65 Ibid., 102 f.

that an international consensus would be required to extend the notion of a prohibited use of force to cyber attacks without direct physical consequences; only cyber attacks targeting the destruction of physical assets or injury of physical persons could qualify as a use of force, while attacks against immaterial property or the functioning of information systems ought to be seen as forms of economic coercion and thus as a potential violation of territorial integrity.[66] A third solution is proposed by Schmitt, who argues that the results of an act ought to be evaluated in order to determine whether they resemble the results of military force or mere economic or political coercion.[67] For this purpose, he suggests undertaking a balancing exercise of seven criteria, which serve as guidance for States to determine whether a cyber attack at issue could fall foul of the prohibition to use force.[68] While a general tendency to focus on the consequences rather than the means employed can thus be identified, there does not yet exist a consensus over the level a cyber attack needs to reach to qualify as a prohibited use of force.

It is even less certain when the level of an 'armed attack', as mentioned in Article 51 of the UN Charter, is reached. This is important because the threshold of an 'armed attack' would open up the possibility for the attacked State to retaliate in legitimate self-defence.[69] For our present purposes of assessing cyber activities in peace-time, it is enough to note that there is an evident lack of a clear 'ceiling' to the notion of prohibited intervention into territorial sovereignty and integrity. As a result, at least at the current state of international cyber law, it remains difficult to clearly set the 'upper limit' for violations of territorial sovereignty and integrity since there is no clear notion of when the prohibited use of force starts. In the next subsection, a number of examples of cyber activities will be discussed, which in State practice are typically not seen as cyber attacks. A third subsection discusses the duties arising for States, with which they have to comply in order to avoid a violation of another State's territorial sovereignty and integrity.

---

66 W Heintschel von Heinegg, 'Informationsrecht und Völkerrecht: Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung' in V Epping, H Fischer and W Heintschel von Heinegg (eds), *Brücken bauen und begehen: Festschrift für Knut Ipsen zum 65 Geburtstag* (C.H. Beck, Munich 2000), 139.

67 MN Schmitt, 'Angriffe im Computernetz und das ius ad bellum' (1999) Neue Zeitschrift für Wehrrecht 177, 183; see also MN Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) Columbia Journal of Transnational Law 885, 911.

68 MN Schmitt, 'The Sixteenth Waldemar A. Solf Lecture in International Law' (2003) Military Law Review 364, 417. Schmitt's criteria are the severity of the consequences; how immediately the consequences occur; the directness of the attack and the consequences, i.e., the extent of the cause-effect relationship between them; the invasiveness of the attack; the measurability of the consequences; the presumptive legitimacy of the action under both domestic and international legal regimes; and the extent to which the State is responsible for the attack. Schmitt insists, however, that the criteria are not 'legal' in the sense that they do not enjoy the same status that e.g. proportionality possesses, MN Schmitt 'The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowski' (2012) 4th International Conference on Cyber Conflict 311, 314-315.

69 See comprehensively on the debate over the notion of an 'armed attack' in cyber space Waxman, 111 ff. See also on the debate over the difference between a mere 'use of force' and an 'armed attack' and the resulting consequences *Tallinn Manual*, 55 para 5 (Rule 13 Self-defence against armed attack).

4.2 Examples of Cyber Activities as Potential Violations of Territorial Sovereignty and Integrity

Leaving aside the notion of the use of force and its complexities in the cyber context, the aim of this section is to consider a number of typical examples of acts that are likely to be considered a violation of territorial sovereignty and integrity. These examples help to subsequently explore under what duties States are to prevent such acts from turning into violations. Centrally, it must be noted that the examples apply under the caveat that there is no clear consensus on whether acts that cause no actual physical damage, such as the use of malware only to monitor activities, can qualify as a violation of territorial sovereignty.[70] Based on the omnipresent focus on coercion noted in general international law,[71] a mechanistic focus on actual damage seems unwarranted. Rather, coercive effect is probably the most helpful benchmark to evaluate each individual case.

As a first example, the easy availability of information through cyberspace could be used by one State to politically influence another. For example, it could provide a safe haven for bloggers critical of their own government, or send political propaganda into that State with the aim of strengthening anti-government forces. Indeed, in general international law Cuba has repeatedly protested that its territorial sovereignty is violated by unauthorised television and radio broadcasts from the United States.[72] However, it remains doubtful whether such actions by States would reach the threshold of coercion identified in the case law of the ICJ. In *Nicaragua*, the Court only identified a violation of territorial sovereignty by intense financial and logistical support given to subversive groups. In all likelihood, in most contexts political influence via cyberspace will thus not constitute a prohibited intervention. The practice of the United States, with its emphasis on the protection of the freedom of speech, is also likely to prevent precedents of a contrary nature. Acts that clearly aim at regime change in another State could, however, be classified as 'coercion' and thus be prohibited. Examples could be the manipulation of elections or of public opinion by cyber means, such as spreading false news, altering online news services in favour of a particular political party in the other State, or attacking the online services of a political party.[73]

Another possible concern is cyber espionage. Intrusions into the computer systems of another State could be undertaken to gain valuable information or to manipulate data. International law generally does not regulate and thus does not prohibit espionage.[74] In fact, if spies are caught by a State, custom and practice is that they can be punished

70 *Tallinn Manual*, 16 para 6 (Rule 1 Sovereignty).

71 See section 2.1.

72 Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/64/129/Add.1 (9 September 2009), 3 para 8. See also Kanuck, 1574.

73 *Tallinn Manual*, 45 para 10 (Rule 10 Prohibition of threat or use of force).

74 Goldsmith, 'Laws of War', 135. For more detail on cyber-espionage, see K Ziolkowski 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in this volume.

by that State, but that if no wrongful act triggering State responsibility has occurred; a violation would have to be based on specific rules of international law such as diplomatic immunity.[75] The same rules arguably apply to cyberspace: intrusions into foreign computer systems are thus not *per se* prohibited, espionage being also a very common practice among States.[76] This finding remains unchanged even where protective barriers such as passwords or firewalls have to be overcome for the purpose of espionage.[77]

As a third related concern, economic espionage follows similar rules. Recent tensions between the United States and China over this issue have shown that, despite the massive economic damage that the United States claims to suffer because of alleged Chinese-sponsored economic espionage,[78] it still does not assert that a violation of international law has occurred.[79]

Fourth, cyber crime is a further cyber activity that could potentially interfere unduly with another State's territorial sovereignty and integrity. Again, States have proven reluctant to imply that obligations stemming from territorial sovereignty and integrity could have been violated if cyber crime strikes in one State but comes from another. Even massive Distributed Denial of Service (DDoS) attacks, which some would qualify as a use of force, are in fact often treated as mere 'crimes' which must be tackled by national criminal law.[80] The Council of Europe *Convention on Cybercrime* is one of the rare achievements of international treaty-making activity in the matter,[81] but it is limited to efforts towards harmonising national criminal laws in the subject area of cyber crime, improving investigation techniques, and furthering international cooperation between national prosecuting authorities.[82] For this purpose, it categorises acts against the confidentiality, integrity or availability of computer services as criminal, but in no way refers to them as cyber attacks constituting a use of force.[83]

---

75 DP Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies' (2013) 17 ASIL Insights 1, 2. See generally on espionage and international law, S Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 Michigan Journal of International Law 1071.

76 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace', 16.

77 *Tallinn Manual*, 45 para 8 (Rule 10 Prohibition of threat or use of force).

78 See, in particular on the massive theft of military intellectual property rights such as the 2007 hack of the 1,4 trillion USD F-35 Joint Strike Fighter project, E Nakashima, 'Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies', *Washington Post* (28 May 2013).

79 Fidler, 3-4, discussing for this purpose the current administration's approach.

80 See, e.g. on the necessary reforms of domestic criminal law in the light of cyberspace, SW Brenner, 'Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?' (2004) 30 Rutgers Computer & Technology Law Journal 1.

81 See, on the UN efforts, in particular the resolutions on creating a 'culture of cybersecurity', Kanuck, 1581.

82 See, on the Convention generally, M Vatis, 'The Council of Europe Convention on Cybercrime' (2010) Proceedings of the National Research Council Workshop on Deterring Cyber Attacks 207, 207 ff.

83 Kastenberg, 55.

Yet another threat arises from cyber terrorism. Due to their effects, acts of cyber terrorism could certainly qualify for some as cyber attacks falling under the prohibition to use force. However, after the 2007 attacks on infrastructure in Estonia, the government preferred to label the attacks as acts of terrorism rather than as a use of force, mainly because the perpetrators seemed to be private citizens rather than the Russian Federation as a State.[84] Given a sufficient component of coercion, while not reaching the level of a veritable use of force, such acts could constitute a violation of territorial sovereignty and integrity. For the case of cyber terrorism, scholars have drawn comparisons with the case of Afghanistan and Al-Quaeda's attack on the United States on September 11th 2001. One could thus impute in a similar way responsibility to a State for the failure to prevent non-State actors from engaging in violations of the prohibition to use force for cyber attacks[85] – and arguably also acts of cyber terrorism below that threshold.

The same considerations also apply to so-called cyber sabotage. One need not necessarily refer to the well-known Stuxnet incident for this purpose; more recently hackers have targeted the computers of the water system of the city of Haifa.[86]

Hitherto, practice seems to point towards no violation of territorial sovereignty and integrity by means of acts of exercising political influence via cyberspace, cyber espionage, cyber crime, cyber terrorism or cyber sabotage. However, a violation could arguably result from any such act that has an intensity which makes it amount to coercion. If a State sees itself forced to change fundamental elements of its political, cultural or socioeconomic system because of interference caused by another State through cyberspace, there could indeed be an act of prohibited intervention and thus a violation of territorial sovereignty. It should be noted at this stage that many such acts could be caused, not by the State itself, but by individuals or groups operating from its territory; attribution is a particularly thorny issue in cyberspace, as will be explored subsequently when discussing State responsibility.[87]

In the light of all this, it becomes imperative to examine to what extent States are obliged to control and regulate cyberspace within the reach of their sovereign powers, in order to avoid being held responsible for breaches of the territorial sovereignty and integrity of other States caused by acts which emanate from their territory.

4.3 Territorial Sovereignty and Integrity and the Resulting Duties for States

Although the potential violations discussed above can of course be committed by the State itself or its authorities, much more relevant in practice are the actions of private

84 Ibid.

85 Kanuck, 1591.

86 'Israel foils Syrian cyberattack on water system, security expert claims', *Washington Times* (25 May 2013).

87 See section 5.1.

parties and the extent to which States are obliged to prevent violations which originate in their territory. As but one example, one can think of the 'patriotic hackers' operating from Chinese cyberspace.[88] At the centre of this discussion of the duties of States must thus be the responsibility to prevent a State's cyberspace from being used for purposes causing a violation of the territorial sovereignty and integrity of another State.

In general international law, a landmark ruling on this topic was handed down by the tribunal in the well-known *Trail Smelter* case. Confronted with cross-border environmental pollution by a factory, the tribunal held that 'under the principles of international law [...] no State has the right to use or permit the use of its territory in such a manner as to cause injury [...] in or to the territory of another or the properties or persons therein, when the case is of serious consequence', and found the State that had not prevented pollution caused by private parties and emanating from its territory responsible under international law to compensate the other State.[89] The ICJ added in the *Corfu Channel* case that every State was under an obligation 'not to knowingly allow its territory to be used for acts contrary to the rights of other States'.[90] There is thus a well-established duty of prevention under international law which concerns criminal acts, but also all other acts that are unlawful under international law[91] and cause sufficiently serious injury on the territory, or to objects, protected by the sovereignty of another State.

The two triggers for the duty of prevention to arise – knowledge and serious injury – must be distinguished from the substantive obligation of due diligence. Starting with the 'triggers', in cyberspace it seems generally acknowledged that serious injury caused to another State as the trigger of the duty of prevention need not necessarily be physical damage, but that other negative effects can be sufficient, too.[92] The second trigger of knowledge requires some more intense consideration.

4.3.1 Triggering the Duty of Prevention: The Role of Knowledge

Both actual as well as constructive or presumptive knowledge can in principle trigger a State's duty to prevent. A State may, for example, have detected a particular problematic activity emanating from its territory; it may have been informed by the victim State; or it can be presumed to know if a cyber activity can reasonably be considered to

88 See e.g. on the Ghostnet system 'Tracking *Ghostnet*: Investigating a *Cyber Espionage* Network', *Information Warfare Monitor* (29 March 2009), 48.

89 *The Trail Smelter Arbitration Case (United States v. Canada)* Reports of International Arbitral Awards, Vol III pp 1905-1982, 1965 (1941). See closer on customary rules of international environmental law and their role for cyberspace regulation by international law T Marauhn, 'Customary Rules of International Environmental Law – Can they Provide Guidance for Developing a Peacetime Regime for Cyberspace?' in this volume.

90 *The Corfu Channel Case,* 22.

91 See *Tallinn Manual*, 27 para 5 (Rule 5 Control of cyber infrastructure) on the notion of unlawfulness.

92 *Tallinn Manual*, 27 para 5 (Rule 5 Control of cyber infrastructure).

belong to a series of such activities.[93] Constructive ('should have known') knowledge is, however, more disputed among scholars in the case of cyberspace. There is currently no consensus if a State violates its duty of prevention where it fails to use due care in policing cyber activities in its territory; in particular, the threshold of such care is difficult to determine because of the ease with which cyber attackers may deceive a State.[94] At least to some extent, the regulatory approach of the State should be taken into account when determining whether constructive knowledge seems plausible. As an example, after recent cyber sabotage attacks on US-based oil, gas and electricity companies, US government officials argued that, despite the fact that the evidence did not permit a definitive conclusion that the acts were sponsored by Iran, control over the internet was so centralised in that country that it was 'hard to imagine' that such acts could be perpetrated without government knowledge.[95]

In the doctrine it has been suggested that, leaving aside the criterion of knowledge completely, the duty of prevention on the State can be based on its actions in general; a State could thus be held responsible if it fails to enact criminal laws or to ensure sufficiently strict law enforcement, or if it displays passiveness and indifference towards problematic cyber activities on its territory.[96] This approach, which assumes the mere theoretical possibility of a State transforming itself into a 'sanctuary' for e.g. cyber criminals, seems to go too far. The ICJ insisted in the *Corfu Channel* case that '[...] it cannot be concluded from the mere fact of the control exercised [by a State] over its territory [...] that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein'.[97]

More plausibly, Heintschel von Heinegg suggests that, instead of such a general presumption, a more limited presumption can apply to the criterion of knowledge. Where a potentially problematic activity has been launched from cyber infrastructure which is exclusively used by the government of a State, a rebuttable presumption can apply that the State should have known of this use of its territory.[98]

Arguably, this proposal can be developed even further for the case of proceedings before an international court or tribunal. The critical issue in this context is arguably the burden of proof. Generally, in international law the principle of *actori incumbat probatio* applies, which requires that the party alleging a fact has to provide proof of its

93 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace', 16.

94 *Tallinn Manual*, 28 para 11 (Rule 5 Control of cyber infrastructure).

95 N Perlroth and D Sanger, 'New Computer Attacks Traced to Iran, Officials Say', *New York Times* (24 May 2013).

96 MJ Sklerov, 'Solving the Dilemma of Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent' (2009) 201 Military Law Review 171.

97 *The Corfu Channel Case,* 18.

98 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace', 17.

claim.[99] If a *prima facie* case has been made, the burden of proof shifts to the other party who now has to refute the claim established by the first party. Presumptions operate here to attribute the burden of proof. Normally, a State alleging that it has suffered a violation of its territorial integrity by non-State actors acting from cyberspace within the territory of another State has to make a rather difficult *prima facie* case showing why the other State knew or should have known about the non-State actors' activities. This would be the trigger to examine and find a violation of the duty of prevention. Based on Heintschel von Heinegg's proposal, it would suffice for the party complaining of a violation to show that exclusive government cyberspace infrastructure was used to start the violation of its territorial integrity. The defending State would then carry the burden of proof to show that the infrastructure in question had, for example, been infiltrated or manipulated and thus it could not be aware of the consequent prohibited actions which resulted. This would seem like a reasonable transposition of the approach taken by the ICJ in the *Corfu Channel* case, where the court held that, based on the reality of exclusive territorial control, a complaining State could benefit from a more lenient standard of proof as regards circumstantial evidence and factual inferences.[100] In the case of cyberspace, the demonstration that exclusive government infrastructure had been used to launch a cyber operation corresponds to the more lenient standard of proof which the complaining State has to meet in order to shift the burden of proof to the defending State.

This solution would ensure that governments have an incentive to protect their essential cyberspace infrastructure, but it does not make it overly easy for other States to bring a successful claim of violation of territorial integrity. At the same time, it must be kept in mind that the criterion of knowledge only serves as a trigger for the duty of prevention; it does not touch upon the question of attribution of the conduct of non-State actors to the State in whose territory they are active.[101]

4.3.2 Substantive Obligations under the Duty of Prevention: The Standard of Due Diligence

The standard of due diligence is widely accepted in the field of prevention of transboundary harm in international environmental law,[102] and arguably also applicable to other potential violations of international law and other damage.[103] The applicable

99 See e.g. G Niyungeko, *La preuve devant les juridictions internationales* (Bruylant, Brussels 2005), 68; M Kazazi, *Burden of Proof and Related Issues - A Study on Evidence before International Tribunals* (Kluwer Law International, The Hague 1996), 221.

100 *The Corfu Channel Case*, 18.

101 See also Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace', 17.

102 See e.g. International Law Commission, *Commentary on the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*, 2001, Report of the ILC on its 53rd Session, A/56/10, 392.

103 See also Interim Report of the Council of Europe Ad Hoc Advisory Group on Cross-Border Internet to the Steering Committee on the Media and New Communication Services, *Incorporating Analysis of Proposals for*

standard is, however, quite flexible and must be adapted to the situation at issue; typically, it will require a behaviour by the State that would qualify as 'good government'[104] and for the State 'to take all appropriate measures at its disposal to prevent and minimise foreseeable significant transboundary harm'.[105]

The concrete obligations in terms of due diligence[106] resulting from the duty of prevention are to be determined in each case. In general international law, these obligations were to a large extent developed in early 20th century arbitral awards, in particular in the framework of the United States/Mexico General Claims Commission. In one well-known case, Mexico was held to be responsible for a violation of due diligence because its police forces had delayed in prosecuting the murderer of a United States citizen.[107] In another, a local mayor failed to restore order when confronted with a violent mob of locals; the Mexican soldiers who subsequently intervened ended up joining forces with the mob to kill three United States citizens. The Claims Commission held that the failure to protect the foreign citizens from the mob and the failure to take proper steps to apprehend and punish the perpetrators constituted a violation of the due diligence obligation.[108] In the later *Lac Lanoux Arbitration*, the arbitral tribunal concluded that in a case where the industrial use of international rivers was at stake and one State's action could impact on the interests of another, consultations and negotiations in good faith were required; each State had to give reasonable consideration to the interests of others, even if good faith negotiations were ultimately unsuccessful.[109] In the case of cyberspace, it seems thus safe to sum up the obligations under the due diligence principle as a duty on the State in question to ensure that criminal legislation is in place to penalise behaviour which could cause a violation of another State's territorial integrity, that crimes are properly investigated, that perpetrators are prosecuted, and that there is appropriate cooperation with the victim-State during the phases of investigation and prosecution.[110]

The resulting steps that a State may be obliged to take in a particular situation are characterised by the concept of 'reasonableness'. If, for example, a harmful cyber attack is being prepared and a State knows about it, such reasonable responses may include

International and Multi-Stakeholder Cooperation on Cross-Border Internet, Strasbourg 2010, 17 para 72.

104 Shaw, 855.

105 Interim Report of the Council of Europe Ad Hoc Advisory Group, 18 para 72.

106 On the notion of due diligence, see R Geiß and H Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention' in this volume.

107 *Janes Case (United States v Mexico)* Reports of International Arbitral Awards, Vol IV pp 82-98, 85 (1925).

108 *Youmans Case (United States v Mexico)* Reports of International Arbitral Awards, Vol IV, pp. 110-117, 116 (1926).

109 *Lac Lanoux Arbitration (France v Spain)* International Law Reports, Vol 24, 101-142, 141.

110 Sklerov, 62.

isolating the network in question.[111] State practice also points in this direction. In 1980, the Soviet embassy in Iran was attacked and devastated by a large group of 'rampaging elements' which also threatened the diplomatic staff. In its complaint, the Soviet Union insisted that Iran had had notice of the impending assault and had therefore failed to take the necessary measures, resulting in a violation of due diligence.[112]

By contrast, the question whether the duty extends to merely prospective acts continues to cause controversy, with some scholars suggesting that reasonable measures to prevent such prospective acts are required. Others deny the existence of such a duty of prevention and point towards the cyber context, where it is extremely difficult, if not impossible, to prepare comprehensive and effective defences against the whole panoply of possible unlawful acts.[113]

One major stumbling block on the road towards a coherent standard of due diligence for cyber regulation arises from the very different attitudes of States towards the topic of cyberspace regulation. Close and intrusive monitoring of cyberspace activity may be a normal activity in some States such as China, but would be anathema to others.[114] To what extent such different constitutional traditions and their effects on cyberspace regulation can be accommodated in an international legal standard of due diligence remains to be resolved. Recent diplomatic tensions point in the direction that, at least for some important players such as the United States, there may be a certain minimum standard of control over cyber activities that needs to be respected.[115]

Another related central element to be taken into account must certainly be the technical feasibility for States to police their borders in cyberspace.[116] Typically, the risk of initial compromise of a government network is virtually impossible to eliminate at the current state of defensive technologies, but limiting the effects and persistence of attacks is much more feasible. As an example, networks or parts of them can be equipped with 'air gaps' for this purpose.[117]

The technical capacity of an individual State is a further aspect that needs to be taken into account when determining the standard of due diligence. This has also been acknowledged in general international law. In the *Sambaggio* decision, the Italy-Venezuela Mixed Claims Commission was asked whether Venezuela bore responsibility

111 The *Tallinn Manual*, 27 para 4 (Rule 5 Control of cyber infrastructure), speaks of a 'self-denial' of service by a State.

112 I Brownlie, *System of the Law of Nations: State Responsibility* (Clarendon Press, Oxford 1986), 119.

113 *Tallinn Manual*, 27 para 7 (Rule 5 Control of cyber infrastructure).

114 Goldsmith, 'Laws of War' 135.

115 Reacting to massive cyber espionage from China, the national security adviser to the President of the United States 'urged China to control its cyber-activity', E Nakashima, 'Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies', *Washington Post* (28 May 2013).

116 Goldsmith, 'Laws of War', 135.

117 The author thanks Kaur Kasak for clarifying these points.

for an injury inflicted on an Italian national by revolutionaries. The Commission accepted Venezuela's contention that a State must only provide protection 'insofar as is permitted by the means at its disposal and according to the circumstances as they may be verified'.[118] It concluded that potential State responsibility, here in the context of revolutionaries as non-State actors, had to be assessed 'in proportion to [… the State's] ability to avoid an evil.'[119]

The contours of the due diligence obligation and the duties incumbent upon States will still require further State practice or even case law from international courts and tribunals to crystallise more clearly. Still, some rough lines can already be drawn based on comparisons with the general state of international law on the matter.

4.3.3 The Duty of Prevention and Transit States

A last problem lies in defining the duty of prevention for States through which data packages are merely channelled for a prohibited intervention in a third State. Some argue that any duty of prevention imposed upon this State will be easily circumvented, since data is always sent in 'packages' which only merge into malicious software at the end of their journey or which can effortlessly be rerouted to nonetheless arrive at their target.[120] However, in the case of an armed conflict which is also conducted by cyber means, a convincing case can be made that a neutral State has an obligation to prevent a cyber attack if it is being mounted through its territory.[121] By analogy, there appears to be no obvious reason why the State should not be under a duty of prevention, as limited as it may be in practice due to technical feasibility, which would have to be taken into account under the standard of due diligence previously discussed.

4.3.4 Other Suggested Regulatory Approaches

Next to the classic rules of international law on the duty of prevention, some scholars also suggest recourse to other approaches which are used in international environmental law to set out the conditions of liability for potentially grave damage caused by accidents from dangerous, but lawful activities.[122] Under international treaties concerning the operation of oil tankers, an obligation to carry comprehensive insurance for harm resulting from dangerous activities is imposed on private operators.[123] For potential damage caused by the civil use of nuclear energy, States decided to reduce insurance costs for private

118 *Sambaggio Case (Italy v. Venezuela)*, Reports of International Arbitral Awards, Vol. X, pp. 499-525, 510 (1903).

119 Ibid., 509.

120 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace' 17.

121 Kastenberg, 56.

122 Kulesza, 144.

123 *International Convention on Civil Liability for Oil Pollution Damage*, Brussels, 29 November 1969, 973 U.N.T.S. 3.

operators by creating a joint liability fund.[124] At the present state of international law with regard to cyberspace, there are no substantive discussions concerning the establishment of such a specific liability regime for cyberspace operators' activities by means of an international treaty.

5. State Reactions to Violations of Territorial Sovereignty and Integrity in Cyberspace

Having established what typically constitutes a violation of territorial sovereignty and integrity, the possible reactions of a State to such a violation should be considered. The starting point is the conditions under which the responsibility of a State for a particular violation is triggered. The following section examines countermeasures which a State might want to employ once a violation of its territorial sovereignty and integrity has occurred. Finally, the possibility for a State to justify its failure to comply with its obligations under territorial sovereignty and integrity by a plea of necessity merits some discussion.

5.1 State Responsibility for Violations of Territorial Sovereignty and Integrity: The Problem of Attribution

Two central conditions must be met for a State's responsibility[125] to be engaged under international law: there must be a violation of a rule of international law, and this violation must be attributable to the State. Damage is not a *conditio sine qua non* for State responsibility unless the rule at issue includes damage as an essential element.[126]

The other issues surrounding a violation of territorial sovereignty and integrity have already been discussed above. There remains, however, the question of attribution of an act to a State, which proves no less difficult to resolve. It should be noted at the outset that in the case of a violation of the due diligence obligation of a State to ensure that its territory is not used for actions violating the rights of other States, inaction can rather easily be attributed to the State. Similarly, State organs or private entities that are empowered by domestic law to exercise 'governmental authority' are also rather straightforward cases in which their action can easily be attributed to the State.[127] The problematic case is thus a different one: difficulties arise where non-State actors violate

124 *Convention on Third Party Liability in the Field of Nuclear Energy,* 29 July 1960, 956 U.N.T.S. 251.

125 See also, on State responsibility, J Klabbers, 'Responsibility of States and International Organisations in the Context of Cyber Activities with Special Reference to NATO' in this volume.

126 *Tallinn Manual*, 30 para 5 (Rule 6 Legal responsibility of States). See also the previous discussion in section 4.1 of what constitutes a violation of territorial integrity as opposed to the use of force.

127 See *Tallinn Manual*, 30 para 6 on the broad notion of 'organs of a State' and 31, para 8 on private entities exercising governmental authority, such as private sector computer emergency response teams in charge of the cyber defence of governmental networks.

another State's territorial sovereignty and integrity, and the role of the State in directing their action cannot easily be established.

Customary international law prescribes that 'the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'.[128] For example, a State might conclude a contract with a private company for certain cyber security tasks; the company's conduct – as far as the State is entitled to give instructions – can thus be attributed to the State. Under the standard of 'control', there has been some controversy in case law.[129] The generally accepted standard is, however, that of 'effective control', under which, for example, support for planning a cyber activity violating the territorial sovereignty and integrity of another State may amount to such a breach if the State is sufficiently involved.[130] Mere financing and the provision of equipment is insufficient; participation in the planning and supervision of activities is required for attribution of the non-State actors' conduct to a State.[131]

Typically, the conduct of 'hacktivists' or 'patriotic hackers' will thus not be attributed to the State. Such individuals or groups commit acts such as intrusions or sabotage by DDoS attacks based, for example, on patriotic motives.[132] Expressing support or encouragement for such acts is also insufficient for attribution.[133] In some rare circumstances conduct may be attributed because a State adopted it as its own.[134] The conditions laid down in the jurisprudence of the ICJ are quite restrictive, require both acknowledgment and adoption of the conduct cumulatively, and more than mere tacit approval.[135]

The central problem in the field of attribution for cyberspace conduct is proof. A scholar describes succinctly the three-level problem of attribution in cyberspace: when back-tracing conduct, a State faces difficulties clarifying 'what computer was used, who

128 Article 8 ILC *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (hereinafter referred to as *Draft Articles on State Responsibility*), General Assembly Resolution 56/83 (12 December 2001), Annex.

129 The International Criminal Tribunal for the former Yugoslavia had established a more lenient 'overall control' test in *The Prosecutor v. Dusko Tadic* Judgment of 15 July 1999, Case No IT-94-1-A, ICTY Appeals Chamber, paras 131 and 145. The International Court of Justice, however, disagreed and insisted that in the field of State responsibility, the test to be applied continued to be that of 'effective control', *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* ICJ Reports 2007, 43, paras 403-405.

130 *Case Concerning Military and Paramilitary Activities in and against Nicaragua,* para 115.

131 *Tadic,* para 145.

132 See also Kastenberg, 59, who describes how a journalist showed how he himself could easily become such a cyber warrior within less than an hour by simply searching and downloading pre-packaged software from the internet, within the context of cyber attacks on Georgia originating in Russia.

133 *Tallinn Manual*, 33 para 11 (Rule 6 Legal responsibility of States).

134 Article 11 ILC *Draft Articles on State Responsibility.*

135 See the well-known example in *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)* ICJ Reports 1980, 3, para 74.

was sitting at the computer (if it's not government-owned), and what government or organisation that person worked for'.[136]

For government cyber infrastructure, matters are even more complicated. Traditionally, the use of State-owned assets such as military equipment can be attributed to the State without much difficulty. In cyberspace, intrusions into government cyber infrastructure by network information modifications such as 'spoofing' – feigning the identity of another organisation or entity – are common phenomena. A different approach is thus required.[137] For good reasons, cyber defence systems typically aim to protect end points, that is, the computers rather than the networks. Experienced cyber attackers are easily able to cover their tracks using compromised hosts within the State under attack, and to intrude into networks via techniques such as watering-hole attacks.[138] Therefore, a cyber operation originating from governmental cyber infrastructure cannot be considered 'sufficient evidence' to attribute said operation to a State, but constitutes merely an 'indication' that the State is 'associated' with the operation.[139]

The means typically employed do not provide much help in answering questions of attribution of conduct to another State either. Most of the technology and software used in this context is of dual use and can easily be reconfigured to serve harmful purposes if desired.[140]

Clearly, establishing State responsibility in cyberspace is an arduous task mainly because of the specificities of cyberspace which make attribution difficult, if not close to impossible in some situations.

5.2 Countermeasures

Based on the customary rules of international law, a State is entitled to react lawfully to a violation of international law by a countermeasure which would otherwise itself violate international law, as long as the requirements applicable to countermeasures are met.[141]

The typical requirements for countermeasures apply just as well for countermeasures in cyberspace. As an example, countermeasures may never be used for punitive purposes, but must only aim at inducing compliance by the targeted State with its international

136 Glennon, 382.

137 *Tallinn Manual*, 35 paras 3-4, (Rule 7 Cyber operations launched from governmental cyber infrastructure).

138 During a watering-hole attack, attackers compromise other networks which the target organisation trusts to then compromise the target organisation. Even rules given out in strict IT environments which allow access only to specified, so-called 'white list' sites can thus be circumvented by such watering hole attacks. The author thanks Kaur Kasak for clarifying these points.

139 *Tallinn Manual*, 34 Rule 7 Cyber operations launched from governmental cyber infrastructure.

140 Heintschel von Heinegg, 'Territorial Sovereignty in Cyberspace', 18.

141 Article 22 ILC *Draft Articles on State Responsibility*. See also on countermeasures MN Schmitt, 'Cyber Activities and the Law of Countermeasures' in this volume.

obligations; and they must only be aimed at the State violating its obligations, and if possible in such a way that the performance of the concerned obligations can be resumed again in the aftermath.[142] As an example, the *Tallinn Manual* describes State B launching a cyber operation against an electricity plant at a dam in State A in order to force that State to increase the flow of water in a river running through both States. State A would thus be entitled to launch a cyber operation against State B's irrigation control system as a countermeasure.[143] State A must, of course, ensure that such a manipulation would not have irreversible effects, such as a severe drought or irreparable damage to vulnerable ecosystems.

There are some further issues that cause concern for countermeasures in cyberspace. As a starting point, countermeasures must not violate the prohibition on the use of force.[144] As previously discussed, there is not yet a clearly established line, either in case law or in doctrine, to delineate cyber attacks from mere violations of territorial integrity.[145] Furthermore, even in general international law, there is continuous debate on the notions of the use of force and an armed attack. Based on Article 51 of the UN Charter, an 'armed attack' can be countered by a State using force in legitimate self-defence. For actions below the threshold of an armed attack, however, there are two positions: a majority would suggest that a State can only resort to non-military countermeasures respecting the prohibition on the use of force; in contrast, a minority opinion, voiced most prominently by Judge Simma in the *Oil Platforms Case*, suggests that a State may react to such low-level violence also with violent countermeasures, so-called on-the-spot reactions.[146]

States thus already face considerable uncertainty in deciding when they are entitled to resort to countermeasures and even when they have decided to do so, things do not become much clearer. As a general requirement, countermeasures must fulfil the requirement of proportionality.[147] What constitutes a proportionate response is, however, not easy to determine. Speaking about the problem of gauging the appropriate response to a cyber attack, Goldsmith notes that a State planning self-defence measures may have a hard time knowing when, and to what extent, to respond in cases where cyber attacks build up slowly and incrementally. Both the exact nature and scale of the attack as well as the consequences can only be estimated at a late stage, if at all.[148] The

142 Article 49 (1), (2) and (3) ILC *Draft Articles on State Responsibility.*

143 *Tallinn Manual*, 37 para 2 (Rule 9 Countermeasures).

144 Article 50 (1) a ILC *Draft Articles on State Responsibility.*

145 See above section 4.1.

146 See *Oil Platforms (Islamic Republic of Iran v. United States of America)* ICJ Reports 2003, 161, separate opinion of Judge Simma, paras 12-13.

147 See e.g. *Naulilaa (Portugal v. Germany)* Reports of International Arbitral Awards (1949), Vol II 1011, 1028; *Case concerning the Gabčikovo-Nagymaros Project (Hungary v. Slovakia)* ICJ Reports 1997, p 7, para 85.

148 Goldsmith, 'Laws of War', 134.

same considerations arguably apply in the case of other cyberspace activities below the threshold of a use of force.

5.3 Necessity

Under customary international law, a State can invoke a defence of necessity to 'preclude' the wrongfulness of actions it has to take because of an emergency situation. As a cyberspace-related example, a State could decide to shut off part of its cyber infrastructure as a protective measure to react to a cyber incident endangering its essential interests, as the only way to protect itself, thereby affecting other States' cyber systems.[149] Another possible example could be a State having to partially let down its guard to focus its cyber defence resources on repelling one particularly threatening cyber attack, thereby violating its duty of prevention.[150] Crucially, the State's action is directed against the danger itself and not against another State or aggressor as in the case of self-defence. Attribution is thus not a central concern where, for example, action is taken against hijacked computer systems without knowing or being able to reach the command and control computer.[151]

Two points should, nonetheless, be highlighted. First, restrictive conditions must be met to invoke a state of necessity. The act to be undertaken must be 'the only way' to protect an 'essential interest against a grave and imminent peril'; it must not 'seriously impair' an essential interest of the other State or States towards which the obligation in question exists or towards the international community as a whole; the obligation at issue must not exclude necessity; and the State must not have contributed to the emergence of the emergency situation.[152]

Second, it is unclear under customary international law what the exact consequences of a preclusion of wrongfulness of the act are. Article 27 (b) of the International Law Commission *Draft Articles on Responsibility of States for Internationally Wrongful Acts* reflects this, stating that the invocation of necessity is 'without prejudice' to the 'question of compensation for any material loss caused by the act in question'. It may thus depend upon the circumstances of the individual case whether compensation for any damage caused will still have to be paid by the State invoking necessity.

6. Conclusion

Cyberspace is neither a *terra nullius* nor a 'fifth dimension' beyond the reach of legal regulation. It is a very real part of the world to which the concept of territorial sovereignty

149 *Tallinn Manual*, 40 para 12.

150 See above section 4.3.2.

151 The author thanks Katharina Ziolkowski for stressing this point.

152 Article 25 ILC *Draft Articles on State Responsibility.*

and integrity of States under international law undoubtedly applies. This brings with it the 'usual' questions, such as how far and in what situations States' jurisdiction may extend beyond their territorial borders.

However, a number of typical concerns in international law are exacerbated by the particularities of cyberspace. The exercise of extraterritorial jurisdiction based on the effects principle may be encouraged by the multitude of cross-border transactions facilitated by cyberspace, leading to more frequent disagreements between States over the legitimacy of individual claims to jurisdiction. Neither is the content of territorial sovereignty and integrity easy to determine; the threshold of when a cyber attack qualifies as a use of force is not yet clarified, and even in general international law there is no clarity of the element of 'coercion' required to turn mere interference with the territorial sovereignty and integrity of another State into a prohibited intervention. It is also particularly difficult to establish the extent of the duty of a State to ensure that no acts by non-State actors violate the territorial sovereignty and integrity of other States; in particular, the degree of due diligence required and the condition of actual or presumptive knowledge a State must possess are yet to be clarified. Even when a State would like to react to a perceived violation of its territorial sovereignty and integrity, it faces the complex challenge of attributing an act committed anonymously via cyber infrastructure with sufficient certainty to another State; of calibrating the moment and intensity of a response in the form of a countermeasure; or of finding the right measure when acting against a grave and imminent peril in cyberspace under a state of necessity.

With these uncertainties of the current state of international law for cyberspace, calls for establishing common rules have emerged[153] and the *Cybercrime Convention* is one of the few achievements in this regard. Others call for the creation of a veritable *ius internet*.[154] Some issues, however, make progress difficult.

Secrecy is a central concern. States are caught between the unwillingness to reveal their potential for cyber activities and the desire to demonstrate said potential to dissuade other States from targeting them via cyber means.[155] Much of what happens in cyberspace remains unknown, which also renders the assessment of State practice for the formation of international law a complex task.[156] Combined with the difficulty in clearly attributing conduct in cyberspace to States, discoverability is effectively very low – which removes a central incentive for States to agree to further the development of common rules.[157] For Glennon, the situation in cyberspace compares very unfavourably with that of the rules of the law of war: the latter rules could only become fully effective

153 Kanuck, 1597.

154 Kulesza, 152.

155 See on this dilemma Glennon, 393.

156 Waxman, 121.

157 Glennon, 385.

because they are underpinned by notions such as fear of retaliation, sanctions by third parties and reputational costs for attackers.[158] One may contend that the expectation of reciprocity also constitutes an important reason for States to comply with international humanitarian law.[159] Nonetheless, secrecy arguably remains a stumbling block on the road to more sophisticated rules of international law.

With uncertain rules, there remains considerable potential for escalation if a conflict between two States emerges.[160] It is also in this light that the current reluctance of States to call cyber activities such as economic espionage violations of international law can perhaps be understood.

With this difficulty in creating consensus-based global rules in the near future in mind, the current mostly doctrine-driven development of international law on territorial sovereignty and integrity in cyberspace finds itself between a rock and a hard place: arguing in favour of overtly strict standards of due diligence for States would force some of them to regulate cyberspace much more intrusively than before. It would require them to abandon their own, perhaps open, approach to cyberspace and information exchange which is often based on constitutional traditions. By contrast, fleshing out the obligations on States under territorial sovereignty and integrity as containing only very vague and limited duties risks encouraging the emergence of cyber safe-havens for non-State actors whose actions other States then have to suffer without being able to address the situation with appropriate remedies of State responsibility under international law.

158 Ibid., 381-382.

159 The author thanks Katharina Ziolkowski for pointing this out.

160 Kanuck, 1596.

Terry D. Gill

Non-Intervention in the Cyber Context

1. Introduction

The principle of non-intervention is, on the one hand, a well-established rule of international law and, at the same time, one which is in some respects controversial and open to various definitions and differing interpretations, depending upon how widely or narrowly it is construed. It reflects the basic notion of sovereignty under international law, and the related principles of respect for the political independence and territorial integrity and inviolability of States. Since it is a reflection of sovereignty, it relates to the right of States to exercise jurisdiction over their territory and abroad within the limits posed by international law and to the relative notion of domestic jurisdiction, or *domaine réservé*, under which States are allowed, within the limits posed by international law, to regulate their own affairs.[1] Since international law is dynamic in terms of its scope of applicability, and many matters which formerly were considered to be wholly or essentially within the internal affairs of States are now, to a greater or lesser extent, regulated by international law, there is no fixed limit as regards what falls within the domestic jurisdiction of States and, correspondingly, what would constitute unauthorised interference in a State's domestic affairs.[2]

The terms 'interference' and 'intervention' are themselves sometimes used interchangeably, but the former may well be wider than the latter if a 'classical' approach to intervention is adhered to, whereby 'intervention' is defined as coercive or 'dictatorial' interference, which would leave non-coercive forms of interference outside the ambit of intervention.[3] Intervention, as used in this sense of 'coercive interference', includes various forms of armed intervention, some of which may be legal, as in the case of an act of self-defence, and this implies that the principles of non-intervention and the prohibition of the use of force, and the exceptions thereto, are also related to the principle of non-intervention, although the latter is wider in scope than the former, since

1 The Permanent Court of Arbitration laid down the basic rule in relation to territorial sovereignty as the exclusive right of a State to exercise the powers of a State within its territory in its award in the *Island of Palmas* case (Netherlands *v* USA) 2 *R.I.A.A.* 829, 838-9 (PCA, 4 April 1928). For a contemporary discussion relating to the scope and status of the non-intervention principle, see, *inter alia,* R. Jennings and A. Watts, *Oppenheim's International Law* (9th ed. Oxford University Press 2008), p.428 *et seq.*

2 The relative nature of 'domestic jurisdiction' was recognised by the Permanent Court of International Justice in its oft quoted *Nationality Decrees in Tunis and Morocco* decision, PCIJ Series B, Advisory Opinion of 7 February 1923, p.24.

3 Jennings and Watts, *op.cit.* n.1, *supra,* p.432. See also the discussion relating to the principle of non-intervention by a group of experts convened at Chatham House which was held 28 February 2007, 'The Principle of Non-Intervention in Contemporary International Law: Non-Interference in a State's Internal Affairs Used to be a Rule of International Law: Is It Still?', available at <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/il280207.pdf>.

it includes intervention which falls short of a use of armed force, but is nevertheless coercive in nature.

Such coercive intervention below the threshold of the use of armed force, or which may constitute a low level use of force, but not one which amounts to an armed attack, can take various forms, and has received comparatively less attention than the use of armed force, especially the use of armed force in relation to human rights violations, often referred to as 'humanitarian intervention'. However, it is nevertheless a topic which raises a number of pertinent questions. These include, in particular, what constitutes illegal intervention, what or who is capable of conducting such intervention (is intervention by its nature a State-to-State phenomenon, or can non-State actors also conduct intervention?), and which legal remedies do States have at their disposal to counteract the effects of an illegal intervention to safeguard their sovereignty and legitimate interests. In the 'cyber context', these questions would translate into which forms of cyber interference could constitute 'cyber intervention', which entities are capable, from a legal perspective, of conducting such cyber intervention, and which remedies, including, in particular, remedies available in the cyber domain, are available to the victim State as a means of addressing and, to what possible extent, counteracting illegal cyber intervention.

Since the principle of non-intervention is multifaceted, and 'intervention' is interrelated with various rules and principles of international law, it is imperative to make an attempt at demarcating the limits of its meaning for the purpose of examining it and also determining how, and to what extent, it can be applied in the context of cyber activities which could constitute cyber intervention. Therefore, for the purposes of this chapter, 'intervention' will be defined as coercive conduct falling below the threshold of a use of force amounting to an armed attack, which is intended to (or has the effect of) violate a State's sovereignty by preventing it from carrying out State functions, and/or preventing it from exercising activities or making choices which it is entitled to engage in or make under international law. It can include both coercive activity not constituting a use of force, and also conduct amounting to a use of force which remains below the threshold of armed attack. Such conduct can include, but is not limited to, various forms of unauthorised territorial intrusion and physical coercion, which, in some cases, may amount to a use of force below the threshold of an armed attack. Addressing these preliminary questions within the context of this working definition is a precondition of examining the possibility of cyber intervention. 'Cyber intervention' will be defined as coercive cyber activity which constitutes and corresponds to any of the above elements contained in the working definition of intervention as set out immediately above. Consequently, only coercive activity in the cyber domain which falls short of the use of force amounting to an armed attack will be addressed here, since both the *ius ad bellum*

and *ius in bello* aspects of cyber warfare in the legal sense have been comprehensively addressed in the recently published *Tallinn Manual*.[4]

This chapter is structured as follows: I will first examine in the following section the legal nature and scope of the principle of non-intervention, and examine a number of types of conduct which could constitute intervention below the threshold of the use of force. Further, the questions of attribution and available remedies to illegal intervention will receive attention. Thereafter, the legal framework relating to (non-) intervention will be applied to the notion of cyber intervention and the questions addressed in the preceding sections will be addressed in order to ascertain how, and to what extent, the legal framework relating to (non-) intervention is transposable to the cyber domain. Finally, the above-mentioned questions will be answered and conclusions will be drawn in relation to the applicability of the legal framework relating to (non-) intervention to the cyber domain.

2. Legal Nature and Scope of the Principle of Non-Intervention

In this section, the legal nature and scope of the principle of non-intervention will be briefly set out. In this context, the questions of which types of conduct could constitute intervention as defined above, which entities are capable from a legal perspective of engaging in or conducting activities which amount to intervention and, correspondingly, which entities are protected by the principle of non-intervention under international law, will all be examined.

2.1 Legal Basis of the Principle of Non-Intervention

The principle of non-intervention is not specifically named in the *Charter of the United Nations* (UN Charter), except with regard to the principle laid down in Article 2(7), that is, without prejudice to the enforcement powers of the Security Council in the

4 M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013). In the manual a distinction was maintained between, on the one hand, forms of coercion which fell below the threshold of a use of force and forms of coercion which constituted a use of force and, on the other hand, uses of force below the threshold of an armed attack and those which did constitute an armed attack, giving rise to the exercise of the right of self-defence (see Rules 10-13 and accompanying commentary at pp.42-61). In brief, the approach taken was that coercive acts below the use of force include acts designed to, or having the effect of, preventing a State to exercise choices which it is entitled to make under international law (see p.44). Acts constituting a use of force below the threshold of an armed attack are those which, in terms of the level of harm inflicted and (intended) consequences, were likely to be characterised as a use of force by the international community on the basis of a number of criteria, but were not severe enough to be categorised as an armed attack, triggering the right of self-defence (see pp.48-51). Uses of force which rise to the level of an armed attack are those whose scale and effects in terms of physical injury, death, damage or destruction rise to a significant level and can be considered as reaching a recognisable level of gravity (see pp.54-56). The Group of Experts was divided on the question whether acts which have severe negative effects not involving physical injury, death, damage or destruction could constitute an armed attack (see p.57). The approach taken in this contribution is that all of these can constitute prohibited intervention, but only acts, either below the threshold of a use of force, or acts constituting a use of force below the threshold of an armed attack will receive attention.

maintenance and restoration of international peace and security, the UN Organization shall not intervene in matters which are essentially within the domestic jurisdiction of its Member States. However, the principle is provided for implicitly in several of its provisions, most notably through the reference in Article 2(1) to the principle of sovereign equality as the guiding principle of the Charter and the UN Organization. In the famous *Friendly Relations Declaration*, which was adopted by the UN General Assembly in 1970, 25 years after the Charter was adopted, as a means of clarifying the primary obligations of States under the Charter, the principle figures prominently.[5] It is also reflected in a number of multilateral conventions, including the *Montevideo Convention*, the *Charter of the Organization of American States*, the *Constitutive Act of the African Union* and the *Treaty of Amity and Cooperation in Southeast Asia* (ASEAN Treaty).[6] It is also included in the *Helsinki Final Act* which, while not a multilateral convention in the legal sense, is a politically binding agreement between the Member States of the Organization for Security and Cooperation in Europe (OSCE).[7] As such, it has a clear basis in international conventions including, indirectly, the UN Charter. Most States are members of one or more of these regional organisations and nearly all States are members of the UN, so that the scope of multilateral treaty obligations referring to the principle is virtually universal.

Alongside this basis in international conventions, there can be no doubt that the principle is reflected in customary international law of a universal character. This is clear both from the fact that the above-mentioned conventions simply refer to it in the sense of recognising and reaffirming it as an existing principle, and also from numerous other indications, including several key UN General Assembly Resolutions, such as the previously mentioned *Friendly Relations Declaration*, decisions by international courts and arbitral tribunals, and in legal doctrine.[8] The International Court of Justice (ICJ) has referred to its status as a rule of customary international law on several occasions including, most notably, in its *Corfu Channel* and *Nicaragua* decisions.[9]

---

5 *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, A/Res/25/2625 (XXV), 24 October 1970. See also Chatham House Document, *loc.cit.* n.3 *supra,* p.3.

6 *Montevideo Convention on the Rights and Duties of States* of 26 December 1936 (Articles 3, 4 and 8); *Charter of the Organization of American States* of 30 April 1948, 119 U.N.T.S. 3 (Articles 1 and 3e); *Constitutive Act of the African Union* of 11 July 2000, 2158 U.N.T.S. 3 (Articles 4a and 4g); *Treaty of Amity and Cooperation in Southeast Asia* (ASEAN Treaty) of 24 February 1976, 1025 U.N.T.S. I-15063 (Articles 2 a, b and c).

7 *The Final Act of the Conference on Security and Cooperation in Europe* (1 August 1975) (Helsinki Declaration) (1978) 14 ILM 1292 (Principles I and VI).

8 See nn. 1, 2, 5 and 6 *supra*.

9 *The Corfu Channel Case* (United Kingdom *v* Albania*,* Merits), *ICJ Reports* 1949, 4, at pp.34-35; *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua *v* United States, Merits), *ICJ Reports* 1986, 14, paras.202-205, at pp.106-108.

2.2 Substantive Content and Scope of the Principle of Non-Intervention

Notwithstanding its dual legal basis and general scope of application, there is no explicit definition of what actually constitutes 'intervention', and what precisely the principle of non-intervention is meant to include. It clearly includes acts constituting the threat or use of force, but is undoubtedly meant to be wider than simply restating the contemporary prohibition of the use of armed force. How much wider is a subject of some debate and, in any event, is not fixed or permanent since, as previously mentioned, the matters which are essentially within a State's domestic jurisdiction are subject to change, and many matters which were formerly considered to be wholly or predominately of domestic concern, are now regulated to a greater or lesser extent by international law. Consequently, one cannot simply provide a categorical list of matters which, by their nature, are covered by the principle of non-intervention as domestic or internal affairs.

However, despite the lack of an explicit definition of what constitutes unlawful intervention and the relative nature of the concept of 'domestic jurisdiction', there is a considerable amount of agreement as to the core meaning of what constitutes intervention, and who or what is the holder of the rights and obligations reflected in the principle of non-intervention. The *Friendly Relations Declaration* refers in its treatment of the principle of non-intervention, *inter alia*, to the use of political, economic or any other measures aimed at coercing a State so that it is prevented from exercising its sovereign rights, or to obtain advantages of any kind. It also refers to action or assistance to subversive, terrorist or armed activities directed at the violent overthrow of the regime of another State, or interference in civil strife in another State. It goes on to stress that every State has the right to choose its political, economic, social and cultural system without interference from other States.[10] This would seem to provide a reasonable indication of the core meaning of the principle, albeit one which is not completely free of ambiguity and a degree of overstatement. For example, while States undoubtedly have a right to choose their particular system of government and pursue economic, social and cultural policies of their own making, this is not an unlimited right. Policies which violate fundamental human rights or which pose a threat to international or regional peace and security are not a matter of free choice, and 'interference in civil strife' at the invitation of a government to assist it in maintaining law and order and in providing a stable environment is widely practiced and accepted as lawful.[11] Likewise, 'the obtaining of advantages of any kind', as stated in the above-mentioned declaration, is potentially misleading and something of an overstatement since, for example, all

10 See n.5 *supra*.

11 See e.g., T.D. Gill 'Military Intervention at the Invitation of a Government' in T.D. Gill & D. Fleck, *Handbook of the International Law of Military Operations* (Oxford University Press 2011), pp.229-232 with accompanying notes on consent as a basis for military intervention. There are numerous controversial examples of allegedly consensual intervention, but the possibility of a State receiving outside assistance to help restore law and order or control over its territory, or resist attempts to forcibly overthrow its government is not widely disputed as such.

States attempt to influence other States to enter into favourable trade and economic relations, and attempt to increase their prestige and influence by means of economic, trade and cultural exchange policies and other forms of cooperation.

Nevertheless, the core meaning of what constitutes unlawful intervention is reasonably clear. It includes action aimed at coercing a State to do, or abstain from doing, something it is entitled under international law to choose to do or abstain from doing. It would clearly include action aimed at overthrowing or undermining the authority of the government of another State, of assisting armed insurrection, terrorist acts, or other similar activities aimed at causing domestic unrest or civil strife. It would also include acts aimed at preventing a State from pursuing its own political, economic and cultural policies, as long as these did not otherwise violate international law, particularly a rule or principle of a peremptory nature, in which case the matter would not qualify as an essentially domestic one. It would additionally include respect for another State's territorial integrity and inviolability, and prohibit incursion or exercise of governmental authority by a State on another State's territory, without that State's freely given and duly authorised consent.

If this is a reasonable, if not necessarily exhaustive, summary of what constitutes unlawful intervention, then it follows that the principle of non-intervention is aimed at not only prohibiting such unlawful intervention, but also at safeguarding the rights of States to exercise their lawful prerogatives and policies, and to maintain their territorial integrity and inviolability *vis-à-vis* other States. It is clear from both the wording and the context of the meaning of the principle of non-intervention, as it is set out in the above-mentioned international conventions, resolutions and judicial or arbitral decisions, that it is primarily directed at *States,* and that the safeguarded rights are those of *States* in relation to each other. Although the principle of non-intervention can also apply to intergovernmental organisations, such as the UN, in the sense of prohibiting them from intervening in the domestic affairs of States, in so far as these are not subject to international law, or otherwise provided for in the constituent instruments governing the relations between the organisation in question and its member States, the *beneficiarie*s of the principle of non-intervention are exclusively States. While international organisations possess a legal personality to a greater or lesser degree, and can enjoy immunities and privileges, there is no corresponding notion of the 'domestic or internal affairs' of such organisations under international law.

Likewise, there is no indication that the prohibition of intervention extends to other entities, such as transnational corporations, armed groups, or individuals. While their actions may well constitute violations of international or domestic law, they do not in themselves, without governmental involvement or assistance, constitute intervention in the international legal sense of the prohibition of intervention, although failure on the part of a State to prevent non-State actors within its jurisdiction from engaging in activities prejudicial to the security and legal order of other States may well result in

State responsibility for failure to act to prevent such harmful activities being conducted from within their territory.[12] Instead of including non-State actors acting on their own within the prohibition of intervention (as either beneficiaries or perpetrators of prohibited intervention), international law makes it possible for States to exercise their criminal jurisdiction in relation to individuals, terrorist or criminal organisations and corporations which engage in activities which undermine their national security or constitutional order or are aimed at disrupting or overthrowing the government of a State, on the basis of the 'protective' or 'security' principle of jurisdiction. This possibility of the exercise of criminal jurisdiction is obviously subject to limitations under international law, and does not extend to either States or international organisations, but exclusively to the exercise by a State of its criminal jurisdiction over persons or, in some cases, criminal organisations or corporations.[13] Moreover, as noted, neither intergovernmental organisations, nor private individuals, corporations, or groups of individuals possess any corresponding notion of 'internal or domestic affairs', which are safeguarded under the principle of non-intervention, although they can benefit from other rights and privileges under international law. In short, intervention is linked to the notion of 'sovereign equality' and is therefore primarily relevant with regard to the relationship between States *vis-à-vis* each other, and additionally, and in a related context, to limiting the right of international organisations to intervene in matters which are not governed by international law, or which are not within the competence of the organisation. It has, therefore, no relevance in relation to acts which are not attributable to States or, where relevant, to an international organisation.

Since, as stated previously, intervention is generally defined as 'coercive' or 'dictatorial' interference, it does not include actions which fall below this threshold. 'Coercion' implies forcible compulsion or restraint and would not include such actions as mere verbal criticism of another State's policies, or moral or even political support for opposition movements, as long as this did not involve incitement or support for attempts to overthrow or undermine or subvert a State's government or its electoral process. It would also not include acts which are otherwise not prohibited under international law, such as diplomatic efforts to obtain more favourable treatment for another State's

---

12 The State-to-State orientation of the non-intervention principle is clearly evident from the multilateral instruments referred to in n.6 *supra,* from the *Friendly Relations Declaration* referred to in n.5 *supra* with accompanying text and from the *Corfu Channel* and *Nicaragua* decisions. In the latter judgement, the Court stated that 'the principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States' (para.205, p.108). The recognition that sovereignty requires a State to abstain from and prevent activities originating from its territory aimed at subverting, overthrowing another State's government or otherwise harming another State's rights, is integral to the principle of non-intervention and was explicitly recognised in the arbitral awards and court decisions referred to in nn.1 and 9 *supra.*

13 See, *inter alia,* American Law Institute, *Restatement (Third) of the Foreign Relations Law of the United States* (1987), Vol. 1, Section 402 (Bases of Jurisdiction to Prescribe), hereinafter referred to as *Restatement*, pp.237-244 at p.240; Harvard Research in International Law, Jurisdiction with Respect to Crime, 29 *American Journal of International Law* (Suppl. 1935, Pt. II), p.435, p.543; M.N. Shaw, *International Law* (6th ed., Cambridge University Press 2008), at p.666 in relation to the protective principle of jurisdiction. On limitations to the exercise of jurisdiction, see *Restatement,* Section 403, pp.244-48.

interests, or for community interests, such as regional stability or humanitarian or environmental concerns, so long as this did not involve actions which were coercive in nature.

A 'borderline' activity which could, but not necessarily always would, constitute intervention is espionage and the (illegal) obtaining of information relating to a State's military or economic capabilities, or its domestic or foreign policy intentions.[14] While espionage is a domestic criminal offence in most States, it is not prohibited as such by international law, nor is there any generally agreed definition as to what constitutes 'espionage' for the purposes of criminal prosecution under municipal law. It is routinely and regularly engaged in by many, if not all States, to a greater or lesser degree. It can violate specific rules of international law, for example, if diplomatic agents engage in 'activities not compatible with their diplomatic status',[15] or involves unauthorised territorial intrusion. Certainly, what is sometimes referred to as 'covert action', in the form of participation in or assistance to military or paramilitary activities or acts of physical sabotage, assassination or abduction on another State's territory, would clearly amount to intervention in the sense of coercive interference. However, in the absence of such acts, the obtaining of information in itself falls short of coercive or dictatorial interference, and would not constitute 'intervention' in the legal sense.[16]

Recently, the disclosure of the massive and systematic use of, *inter alia,* cyber techniques to intercept, monitor and store the email and telephone communications of private citizens, corporations, governmental and intergovernmental organs by the intelligence agencies of certain States, in particular the United States and the United Kingdom, has received significant negative attention in the media, triggered diplomatic protests, and caused tensions between erstwhile friendly nations. The disclosures of such programs as 'Prism' and 'Boundless Informant' give rise to several questions which are relevant within the context of this contribution on cyber intervention.[17]

The main questions in the context of our topic is whether such practices violate international law in themselves, and whether they constitute a form of coercive

---

14 See K. Ziolkowski 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in this volume, sec. 2.1.

15 The phrase is often used when declaring a particular diplomatic agent *persona non grata* on the basis of suspected espionage, cf Article 9 of the *Vienna Convention on Diplomatic Relations* of 18 April 1961, 500 U.N.T.S. 95.

16 See Tallinn Manual, *op.cit.* n.4 *supra*, p.30. See also D. Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies', *ASIL Insights* (Vol.17, Issue 10, 20 March 2013), available at <http://www.asil.org/insights130320.cfm>.

17 Reports on the two programs were released in the *Washington Post* and *Guardian* newspapers and *Der Spiegel* news magazine in June and July 2013. See Glenn Greenwald & Ewen MacAskill, 'Boundless Informant: the NSA's secret tool to track global surveillance data', *The Guardian* (11 June 2013), available at <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>, and Barton Gellman & Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program' *The Washington Post* (6 June 2013), available at <http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers>, as well as the following note (18).

interference which rises to the level of prohibited intervention. Before going into these questions, it is necessary to point out that much of what is reportedly going on is still not in the public domain, and that there are many more issues involved in relation to these reports than simply whether that which has been made public does, or does not, constitute a form of prohibited intervention in the domestic affairs of various States under public international law. However, as one can only work with that which has been made public, and this piece is devoted to the specific topic of intervention in the cyber context, I will restrict my comments accordingly.

From the reports available at the time of writing this contribution, it would seem that both programs are primarily related to the massive and systematic retrieval and storage of information for purposes of surveillance and monitoring activities taking place within and outside the jurisdiction of the United States.[18] It allegedly includes the capture of hundreds of millions of data elements from both internet activity and telephone communications, in a large selection of countries. It also allegedly includes specific acts of further-going espionage, such as the tapping of communications of official governmental agencies of various countries and the diplomatic premises of the European Union (EU) in the United States. While the 'Prism' program seems to be primarily concerned with communications to and from the United States, the 'Boundless Informant' program apparently goes several steps further in capturing, storing and monitoring vast amounts of data from telephone and internet communications which take place wholly outside the jurisdiction of the United States including, allegedly, communications by foreign governments and international organisations, many of which are close allies of the United States.

The existence of such programs confirms that cyber means of surveillance exponentially increase the ability of a government, such as that of the United States, to conduct espionage on foreign States and their citizens at a hitherto unprecedented level. This may well violate the domestic law of the States concerned and, in some cases, constitute not only an arguably unfriendly act, but one which violates the targeted State's sovereignty, in so far as it involves intercepting governmental communications, or those which are otherwise protected under international law, such as the alleged violation of the diplomatic immunity of the EU Mission in Washington. It raises potential issues under international human rights law in so far as data regarding private persons is made available to governmental agencies by technology companies, such as Microsoft, Google and Facebook, which could violate their right to privacy. However, such data retrieval and surveillance does not, in itself, constitute 'intervention' in the sense of coercive interference, except possibly in the situation that governmental offices or diplomatic premises are violated or diplomatically protected communications are intercepted and

[18] See e.g., *Der Spiegel* Nr. 27, 1/7/2013 'Angriff aus Amerika', Cover page article by Laura Poitras, Marcel Rosenbach, Fidelius Schmid, Holger Stark & Jonathan Stock, pp.76-80, and *The Economist* 'Sense, Sensibilities and Spying' article by David Parkins, 6-12/07/ 2013, pp.51-2.

stored. Even in such cases, it is not necessarily the case that any violation of diplomatic immunity or sovereignty would automatically constitute 'coercive interference' amounting to intervention, although it could otherwise be in violation of international law relating to respect for other States' sovereignty and to diplomatic missions. It would depend on how such a violation took place and whether the data retrieved was used to interfere with the targeted State's conduct of foreign relations, or to unlawfully exercise jurisdiction over foreign corporations or nationals.

3. Attribution of Conduct Constituting Prohibited Intervention and Possible Remedies

In this section, the question of attribution of conduct constituting a violation of the non-intervention principle will be briefly examined on the basis of the *Draft Articles on Responsibility of States for Internationally Wrongful Acts*[19] of the International Law Commission (ILC), followed by a discussion of the remedies available to States under international law when faced with an act or acts of unlawful intervention. In that context, primary attention will be focused upon acts of intervention, and remedies thereto, which fall short of a use of force, although secondary attention will be given to certain forms of intervention and related remedies which are at the 'dividing line' between forcible and non-forcible acts.

3.1 Attribution of Acts

The basic notion of international responsibility is that acts or omissions which breach specific rules of international law, such as the prohibition of intervention, engage the responsibility of the State which has violated the rule in question, provided the act or omission in question can be attributed to that State. The illegal character of intervention as set out in the preceding section is not disputed and is uncontroversial from a legal perspective. However, attributing alleged acts constituting prohibited intervention may not always be straightforward. There are some forms of intervention which will be readily attributable to a particular State, as in the case of unauthorised territorial incursion by another State's armed forces. In such cases, it will usually be clearly apparent which State is responsible. However, there are probably many more modalities of coercive interference, where establishing a clear link with a State will be considerably more difficult. This will be especially true in cases of covert intervention below the threshold of the use of force. Many forms of cyber activity which constitute a violation of another State's sovereignty, which cause significant harm to another State's economic interests, or otherwise constitute an interference in another State's internal affairs, would, in many cases, be extremely difficult to prove a sufficient link with a

[19] A/Res/56/83, 12 December 2001, annex.

State necessary to attribute the act in question to a particular State.[20] Some, but by no means all, of these types of covert cyber activity could constitute intervention, provided the threshold of 'coerciveness' was crossed in the sense referred to in the previous section. For this to be the case, the activity in question would have to go beyond mere collection or even theft of data or interception of communications in most cases to fall within the rubric of coercive intervention. If, for example, a State engaged in activity which caused significant economic damage by interfering with banking activities or manipulating the stock market in another State, this would almost certainly constitute coercive interference and, as such, would qualify as prohibited intervention. However, in order to be able to establish responsibility on the part of another State, it would be necessary to prove that such acts were carried out by a State agency, or by private persons, groups of persons or corporations acting under the control or direction of a State agency.[21] Additionally, responsibility would ensue if such acts were conducted by private persons or groups of persons acting on behalf of the State in the absence of official State authorities, or which was subsequently adopted by a State after being committed by private persons.[22]

The rules regarding attribution of internationally wrongful acts are laid down in Chapter II of the above-mentioned ILC's Articles on State Responsibility. These rules, as summarised above, provide the basis for determining whether a breach of an international obligation can be attributed to a particular State, and would therefore be the key in determining whether a particular act of (cyber) intervention could be attributed to a State for the purposes of obtaining redress and compensation. In any such situation, the burden of proof will rest upon the State making the allegation of illegal conduct constituting prohibited intervention.[23] In fact there would be a double burden of proof. Firstly, to establish that the conduct in question did in fact constitute a violation of the non-intervention rule and, secondly, to establish that the conduct could be attributed to a State. As pointed out in the preceding section, intervention pertains solely to activity carried out by a State in relation to another State. Consequently, even

20 A well-known example of cyber interference which caused a degree of inconvenience and temporary disruption of governmental and financial activities was the 2007 DDoS 'attack' on Estonia. While this may have met the threshold of coercive interference, albeit it was of a somewhat limited nature, it has never been definitely established that the acts concerned were conducted by a State (Russia), or by persons acting under the control or direction of a State, rather than by 'patriotic hackers' acting on their own volition, despite suspicions of State involvement. In the absence of proof of attribution, the acts concerned do not constitute a violation of the principle of non-intervention. See e.g., <http://blogs.law.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism>. For a contrary opinion, see R. Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', 17 *Journal of Conflict and Security Law* (2012) 211, pp.218-19.

21 See Articles 4, 5 and 8 of the Draft Articles on State Responsibility (DASR) n.19 *supra*.

22 Articles 9 and 11 DASR, n.19 *supra*.

23 It is a general principle of law, which holds in all main legal systems, that the party making an assertion must provide proof for it (*actiori incumbit probatio)* referred to by Vice-President Wolfrum in his separate opinion in the MV *Saiga* decision, Case no.2 (Merits), 1 July 1999, para.7 of the International Tribunal for the Law of the Sea (ITLOS), available at <http://www.itlos.org/fileadmin/itlos/documents/cases/case_no_2/merits/Separate.Wolfrum.01.07.99.E.pdf>.

if the acts were particularly harmful and constituted a clear case of interference in the domestic affairs of another State, they would not constitute intervention unless it could be proven that they were carried out by a foreign State's agents, or by private persons, corporations or organisations acting 'under the direction or control' of another State. While there is no universally agreed 'law of evidence' in international law, decisions by most courts and tribunals point to a fairly high burden of proof to establish responsibility.[24] That would probably mean in the absence of an admission on the part of the intervening State, or other clear and convincing proof, such as that which has been divulged in relation to the espionage activities of the United States against a number of its allies by a former agent of the agency conducting those activities, that it would be difficult in many instances, if not necessarily always impossible, to make out a case before an international court or tribunal relating to various forms of cyber interference, some of which could constitute prohibited intervention. While the standard of proof in establishing a link of attribution of coercive conduct constituting intervention is not so high as that for establishing criminal liability which requires proof beyond a reasonable doubt, it would be necessary to make out a reasonably clear and convincing case that a particular State was the author of the acts constituting intervention, or had directed or controlled activities by private persons which met that threshold, if the injured State were to undertake countermeasures or have a realistic chance of bringing a successful claim. That brings us to the question as to which remedies are available to an injured State.

3.2 Available Remedies

There are three basic types of remedies available to States who have been or are being subjected to unlawful intervention and interference in their domestic affairs, aside from the right of self-defence in response to an armed attack, which falls outside the scope of this chapter. The first type are measures of law enforcement relating to illegal activities carried out by individuals, groups of persons or corporations. These are based on the right of States to exercise (criminal) jurisdiction over natural persons and other non-governmental entities which violate their domestic law, including activities aimed at undermining the State or interfering with its essential security interests and financial

[24] On the lack of a general law of evidence and the relatively high burden of proof in international law, see T.D. Gill & P.A.L. Ducheine, 'Anticipatory Self- Defense in the Cyber Context', 89 *International Law Studies* (US Naval War College 2013), p.438, pp.451-52 (with accompanying notes), available at <http://www.usnwc.edu/getattachment/f041ec70-19af-4df4-bf59-be73ec0fe493/Anticipatory-Self-Defense-in-the-Cyber-Context.aspx>. Each international court or tribunal establishes its own standards or rules and these vary significantly between them, and even between cases before the same tribunal. The classic, if now somewhat outdated, work on the topic is by D.V. Sandifer, *Evidence Before International Tribunals* (PAIL Institute, Washington DC, rev. ed. 1975). See also separate opinion of Vice-President Wolfrum, referred to in the preceding note where he states in paragraph 4, 'International jurisprudence does not provide for extended guidance in respect of the appreciation of evidence. Contrary to municipal law, international law, in general, and the rules of international courts and tribunals, in particular, have only developed regulations on procedural aspects concerning the submission of evidence by the parties but not on the appreciation of evidence, in general'.

solvency. The 'protective' or 'security' principle of State jurisdiction, referred to above, is recognised under customary international law and enables a State to criminalise conduct aimed at undermining or overthrowing a State's government, or counterfeiting its currency or official documents, or otherwise seriously undermining its financial solvency, even if such acts are conducted by foreign nationals located outside the State's territory. Assuming the suspected perpetrator is present on the injured State's territory, either as result of being arrested while engaged in or subsequent to a criminal act on the State's territory, or by means of extradition, the suspected person(s) could be prosecuted under the domestic law of the injured State for such activities. This would also apply to State agents, for example, foreign intelligence agents, for engaging in activities amounting to intervention or unlawful interference, such as espionage or sabotage, unless they were protected by diplomatic or State immunity under international law.[25] Additionally, other principles upon which the exercise of jurisdiction can be based, such as the (objective) territorial principle, (passive) nationality principle, or 'effects doctrine', might be relevant and applicable, in so far as they are generally recognised under international law.[26] However, only activities engaged in by States or 'under the direction or control of a State' qualify as 'intervention' and, in many cases, this could pose a significant barrier to exercising criminal jurisdiction, since it would be difficult in most cases to identify or prosecute a particular State agent as perpetrator, unless he or she was apprehended on the injured State's territory, and it would be usually impossible to proceed with a criminal investigation in the absence of exercising physical custody over the suspect without cooperation on the part of the intervening State, which is hardly a likely eventuality. Likewise, the principle of sovereign immunity, or in some cases diplomatic immunity (if the suspected foreign agent had diplomatic status) would, in many cases, pose a significant obstacle to proceeding with a criminal investigation or prosecution of foreign State agents or officials who might be implicated in activities amounting to illegal intervention, assuming they held official positions in the government of a foreign State. Moreover, even if sovereign immunity was not relevant, such activities, while illegal under the law of the injured State, might not constitute criminal offences under the law of either the intervening State or third States, in which case possibilities for extradition would be limited or unavailable. Neither

25 An example of prosecution of foreign State agents for illegal activities constituting intervention is the well-known *Rainbow Warrior* case, which involved the arrest and conviction of two French military intelligence agents by New Zealand for causing the sinking and loss of life of one person on board of the Greenpeace vessel, *Rainbow Warrior,* in Auckland harbour in 1985. The incident was mediated by the UN Secretary General and went to arbitration after the terms of the settlement were allegedly violated by France. For the arbitration, see *Rainbow Warrior* Arbitral Award (1990) XX *R.I.A.A.* pp.215- 284. In that case, while the foreign agents were apprehended by the New Zealand authorities and pleaded guilty to criminal charges of manslaughter, they were subsequently released into French custody as part of a political arrangement. However, in many cases the prosecution of suspected foreign State agents does not take place, either because they are not within the territorial jurisdiction of the injured State, or for other reasons, including lack of sufficient evidence for criminal prosecution or official status of the suspected agents.

26 See sources cited in n.13 *supra.*

would such acts be likely to rise to the level of international crimes under universal jurisdiction, thereby precluding prosecution by either third States or by international criminal tribunals, since espionage rarely, if ever, involves participation in recognised international crimes, such as crimes against humanity, war crimes or genocide, which would make the suspects subject to universal jurisdiction.

The second basic type of remedy available to a State confronted with unlawful intervention or forms of interference which fell below the threshold of 'coerciveness' required to constitute unlawful intervention, but nevertheless was either otherwise unlawful under international law (e.g., as violating diplomatic immunity), or which could be regarded as unwarranted or unfriendly interference short of intervention, is recourse to forms of retorsion (also spelled 'retortion') by the injured State in response to either unlawful or unfriendly acts by another State.[27] Retorsion differs from reprisals, nowadays usually referred to as countermeasures, by the fact that the retaliatory measures taken do not otherwise violate international law. Retorsion can take many forms, ranging from placing restrictions on trade, expelling an offending State's diplomatic agents, recalling an ambassador or even breaking off diplomatic relations, or the freezing or terminating of various forms of assistance or cooperation. Also included would be the forcible exercise of rights under international law, including measures which involve the limited threat or use of armed force below the threshold of self-defence, such as intercepting unlawful aerial intrusion by foreign State aircraft, safeguarding territorial waters from non-innocent passage or unlawful incursion into internal waters, or affirming the right of free navigation in international waters in reaction to unlawful or unfriendly attempts to interfere or unlawfully prevent the lawful exercise of such rights.[28] It is, in short, a form of lawful self-help and, as such, may be resorted to in reaction to either unfriendly or unlawful acts, including intervention, by another State.

The third general type of remedy in reaction to unlawful intervention is the carrying out of countermeasures.[29] The purpose of a countermeasure is to secure an end to unlawful conduct and, additionally, to secure a peaceful settlement and reparation, or failing

---

27 For a definition of retorsion see <http://oxfordindex.oup.com/view/10.1093/oi/authority.20110803100416821>. See also E. Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational Publishers 1984), p.5.

28 For a more detailed discussion of retorsion as a form of self-help, see M. Noortmann, *Enforcing International Law: From Self-help to Self-contained Regimes* (Ashgate 2005). For a discussion of forcible measures of retorsion, see T.D. Gill, 'The Forcible Protection, Affirmation and Exercise of Rights under Contemporary International Law', 23 *Netherlands Yearbook of International Law* (1992), pp.105-173. It should be stressed that acts conducted by a State to protect its territory from unlawful incursion not amounting to an armed attack, or to secure rights based on international conventions and/or clearly established customary rules against unlawful interference, such as freedom of navigation on the high seas, even if they include a measure of military force, should not be confused with 'countermeasures'. The distinction is important, as armed countermeasures are prohibited under contemporary international law. By contrast, a State has a clear right to safeguard its territory from unlawful incursion and no question of preclusion of the wrongfulness of such a measure arises, which is why they qualify as measures of retorsion. The reasons for this position are set out in more detail in the last-mentioned source cited.

29 See also M.N. Schmitt, 'Cyber Activities and the Law of Countermeasures' in this volume.

that, to inflict a proportionate degree of retribution upon the offending State. Unlike retorsion, countermeasures (or reprisals) are measures which violate a legal obligation owed to the offending State, but which are not unlawful, provided certain conditions are met. These include a prior demand of cessation of the illegal conduct and redress, unless this would be clearly pointless under the circumstances, a reasonable degree of proportionality, both in qualitative terms (i.e., the countermeasure must primarily be directed towards inducing the offending party to cease its unlawful conduct and provide reparation), and in quantitative terms (the amount of injury inflicted upon the offending party must not greatly exceed the consequences of its unlawful conduct). Additionally, countermeasures may not be directed against individuals in violation of fundamental human rights or humanitarian law, or otherwise violate a peremptory norm of international law, including the prohibition of the use of force in international relations.[30]

While all three of these basic remedies are potentially available and have a role to play in securing compliance with the law and protecting a State's interests when confronted with unlawful interference and intervention, none of them are a panacea and all of them are far from being always effective, either as a deterrent or as a remedy. This is arguably likely to be even more true in the case of (usually covert) cyber interference or intervention than in 'classic' scenarios of unauthorised physical intrusion, as in the unauthorised penetration of Swedish territorial and internal waters by Soviet submarines during the Cold War, or manifest support by a State for armed groups, such as the support of the United States of the *contras* in the Nicaragua dispute, or the involvement of State agents in acts of physical sabotage, as in the *Rainbow Warrior* incident, when French intelligence agents were caught 'red handed' on New Zealand territory.[31] In these types of situations, denial by the perpetrating State is scarcely a viable option and attribution of the acts to a particular State is therefore fairly straightforward. Moreover, acts of

30 The classic case relating to reprisals is the *Naulilaa* Arbitral Award (Portugal *v* Germany) (1928) 2 *R.I.A.A.* 1011, which restated the basic conditions attached to the taking of reprisals. These have been echoed in more recent case law, such as the *Air Services Agreement* Arbitral Award (US *v* France) (1978) 18 *R.I.A.A.* 417, and the *Gabćikovo- Nagymaros Project* (Hungary *v* Slovakia) Judgment, *ICJ Reports* 1997, 7, paras.82-85, pp.55-56. The ILC dealt extensively with countermeasures in its above-mentioned work on State responsibility. See DASR, n.19 *supra* (Articles 22, 26 and 49-54, with accompanying commentary).

31 With regard to the penetration of Swedish territorial and internal waters by submerged foreign submarines in the 1980s, see, e.g., S. Lohr, 'Soviets and Swedes Sparring Over Submarines', in *New York Times* (14 January 1988), available at <http://www.nytimes.com/1988/01/14/world/soviet-and-swedes-sparring-over-submarines.html>. For a legal discussion of Swedish measures to halt violation of their territory see, *inter alia,* Gill, *loc. cit.* n.28 *supra*, at pp.136-140. The US support for the *contra* rebels was a matter of public record and was deemed to constitute unlawful intervention by the ICJ in the *Nicaragua* decision in paras.240-241 of that judgment. The *Rainbow Warrior* incident is discussed above in note 25 and accompanying text. The Algiers Accords of January 1981 brought the Tehran Hostages crisis to an end with the release of the diplomats taken hostage in exchange for the unfreezing of a portion of Iranian assets in US banks and the establishment of the Iran US Claims Tribunal to adjudicate claims connected to the Iranian Revolution utilising the balance of the frozen assets to award compensation. See, e.g., Gary Sick, 'The Carter Administration', in *The Iran Primer: Book Overview,* United States Institute for Peace, available at <http://iranprimer.usip.org/resource/carter-administration-0>.

retorsion in such classic cases of intervention (such as forcing submarines to the surface under certain circumstances) or countermeasures (as in the reaction of the United States to the takeover of its embassy in Tehran, which took the form of freezing very sizeable Iranian assets in United State banks and their overseas subsidiaries), or prosecution of individuals (as in the *Rainbow Warrior* incident) were both feasible and likely to be effective. In a subsequent section, I will examine the extent to which analogous measures in the cyber context would be feasible and compatible with the existing legal framework for taking remedial action under international law. To the extent they are, they could go some way towards providing a remedy for unlawful intervention, albeit an imperfect one in many cases.

4. Application of the Legal Framework to Cyber Intervention

Having set out the applicable legal framework and available remedies, it is now time to attempt to apply it to the phenomenon of cyber intervention. In doing so, I will first discuss what forms cyber intervention might take and distinguish it from other forms of illegal cyber activity. Secondly, I will briefly review some of the best known examples of alleged cyber intervention and discuss what lessons can be drawn from these in relation to realistic possibilities for taking effective remedial action and present some ideas on how States might be able to act in situations below the threshold of reacting to an armed attack and being party to an armed conflict to safeguard their essential interests in conformity with international law.

4.1 What is Cyber Intervention and Which Forms Could It Take?

Our starting point is that cyber intervention is a violation of the principle of non-intervention which is carried out wholly, or at least predominately, in the cyber domain. Consequently, it must rise to the level of illegal coercive activity which attempts to prevent a State from conducting its domestic affairs and foreign relations in conformity with its own choices within the limits of international law. Since we are only dealing with forms of coercion below the threshold of the use of force rising to the level of an armed attack, any act which causes more than minimal damage, physical destruction, physical injury, or loss of life will remain outside our definition and discussion.[32] Hence, acts carried out in reaction to any significant use of force, or within the context of participating as a party to an armed conflict, will be excluded. At the other end of the scale, acts constituting illegal interference which lack the element of coerciveness necessary to constitute 'intervention', such as engaging in espionage consisting wholly of (illegally) obtaining and monitoring information from digital sources from foreign governments, corporations or private individuals, would not, in most cases, constitute 'intervention'. Finally, only acts performed by a State agency, or under the

[32] See definition of use of force n.4 *supra*.

control or direction of State agents, whether civilian or military, would qualify as 'intervention'. Consequently, cybercrime, illegal hacking, cyber corporate espionage and other acts in the cyber domain performed by private or corporate entities not under governmental control fall outside the context of cyber intervention (see section 2.2). Likewise subversive or terroristic (cyber) activities engaged in by more or less organised movements operating without significant State involvement or support would not qualify as 'intervention', although their effects could be similar in some cases (see section 2.2). This leaves a clearly defined and relatively narrow field of activity open to examination and discussion, but one worthy of separate consideration nevertheless.

When turning to what forms cyber intervention could take, it is also important to emphasise that intervention as defined in this chapter has not been a particularly common phenomenon in the physical domain since the end of the Cold War (as opposed to non-coercive forms of espionage and intrusion which are fairly routine occurrences), as an examination of recent State practice and relevant case law would seem to indicate. There are only a relatively limited number of cases and known incidents relating to alleged violations of the principle of non-intervention in the past 20 or so years which meet the conditions set out above.[33] This is probably due to a number of reasons, including, but not limited to, the illegal nature of such action. The most important of these is probably the major transformation of the international system that has occurred since the end of the Cold War, which makes the attempted overthrow or subversion of foreign governments through coercive intervention less likely as a policy option. Alongside this paradigm shift from a bipolar system engaged in ongoing confrontation to a much looser and more interdependent system, other reasons include the fact that the potential costs of illegal intervention usually outweigh any perceived benefits, that undermining or (assisting in) overthrowing a foreign government is usually neither easy, nor free of risk, and is generally only engaged in by a relatively small number of States, which have both the capacity to undertake such action and compelling reasons to do so, without exposing themselves to the possibility of retaliation in one form or another. Assuming this assessment is generally accurate, there are probably no overriding reasons to assume that cyber intervention is, or is likely to become, any more prevalent. Although, it is, perhaps, somewhat easier to conduct intervention in the cyber domain without immediate fear of detection, it is also probably true that any intervention on a significant scale is likely to be either detected or exposed within a reasonable amount of time and then the same considerations relating to the weighing of its potential or perceived

[33] During the Cold War, both the US and the former USSR frequently engaged in intervention in the form of covert action, economic and political coercion of unfriendly governments, support for armed opposition groups and other forms of intervention short of the direct use of military force in attempting to maintain and expand their respective 'spheres of influence'. However, since the end of the Cold War, there have been relatively many fewer documented cases of such activities of State-conducted coercive intervention below the threshold of the use of force. Instead, there has been a proliferation of transnational and internal conflicts based on ethnic, religious and other causes, sometimes leading to (virtual) State failure, alongside the increased potency of various non-State actors, which are the primary security concern at present.

utility and the potential costs involved once reasonable suspicion fell upon a particular State, which was both willing and able to engage in such intervention, would not differ significantly from those relating to more conventional forms of intervention.

Cyber intervention, like its physical counterpart, could take various forms and reach varying degrees of intensity. It could include various forms of misinformation and propaganda aimed at undermining a foreign government's legitimacy and escalating to incitement and coordination of subversive activity, with the purpose of aggravating civil unrest or even overthrowing a foreign government. The (mis)use of social media, email and digital telephone communications for such purposes could be a potentially powerful instrument in inciting or assisting opposition to an unfriendly foreign government, especially in countries which were subject to significant civil unrest as a result of political, social or other types of instability. It could be used to manipulate or influence the outcome of elections in States where polling was (partially) conducted through digital voting procedures. It could be used to break into sensitive governmental and other critical websites with the purpose of interfering with governmental communications, manipulating key economic and financial activities, or planting malware designed to degrade or shut down essential governmental and other key services at a moment of the intervening State's choosing. Such activity could result in the undermining of public and corporate confidence in the ability of the government to maintain essential services, economic stability and public order, without necessarily rising to the level of a use of force, including one which amounted to an armed attack. Large scale and coordinated direct denial of services (DDoS) 'attacks' on governmental and other key economic or financial websites, while constituting a rather crude and blunt instrument, could hamper or even paralyse governmental activity for a shorter or somewhat longer period of time and, in certain situations, could have a significant impact upon the target State, albeit usually of rather limited duration. Cyber intervention could also rise to the level of sabotaging chosen installations resulting in a measure of physical damage, such as a defence communications network, a nuclear research facility, or a particular weapons system, in which case it would approach or cross the threshold of a use of force and, in some cases, could potentially amount to an armed attack. This list is indicative and by no means intended to be exhaustive. Some of these activities have already been engaged in and have been publicly reported, such as the DDoS 'attack' on Estonia which, had it been proven to be controlled or directed by a State, would have been a clear case of prohibited intervention below the threshold of a use of force.[34] Another example which has already occurred and received a large degree of public notoriety is the 'Stuxnet' operation, which apparently resulted in a limited measure of physical damage to Iranian

[34] See n.20 *supra*. For a good general treatment of the Estonia 'cyber attack', see E. Tikk, K. Kaska & L. Vihul, *International Cyber Incidents: Legal Considerations* (NATO CCD COE 2010), pp.14 -34.

nuclear centrifuges and reportedly slowed down its nuclear research programme by several months.[35] It deserves some additional comment.

The 'Stuxnet' operation met all the classical requirements for qualifying as 'intervention'. It was coercive in that it was aimed at preventing a State from pursuing a particular course of action (whether or not it was a legal course of action is another matter). It was clearly conducted by a State (or States acting in cooperation), rather than a group of individuals and it remained below the threshold of an armed attack, since it did not result in either human casualties or significant long-term damage, or disruption of critical infrastructure which was vital for the functioning of the State. It may well have qualified as a use of force (short of an armed attack) in that it reportedly caused a degree of material damage and was intrusive enough to possibly be viewed as a use of force by some commentators, although the Iranian Government has downplayed its effects and has not claimed it was a use of force, or an armed attack.[36] Whether or not it was a legal form of intervention is an open question. On the one hand, it clearly and coercively interfered with a State's chosen domestic policy and temporarily prevented it from carrying out nuclear research for avowedly peaceful purposes. On the other hand, there are serious doubts regarding the purely non-military nature and intentions of Iran's nuclear policy, and clear indications that Iran is acting in violation of the *Treaty*

35 See, *inter alia,* Buchan, *loc.cit.* n.20 *supra*, pp.219- 221; D. Sanger, 'Obama Order Sped Up Wave of Cyber Attacks Against Iran', *New York Times* (1 June 2012), available at <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0>. For the present author's opinion as to why it did not constitute an armed attack, see Gill & Ducheine, *loc.cit.* n.24 *supra*, p.459.

36 *ibid.* For speculation as to the legal nature of the Stuxnet attack, see P. Rosenzweig, *Lawfare* blog (2 June 2012), available at <http://www.lawfareblog.com/2012/06/the-stuxnet-story-and-some-interesting-questions/> See also D.P. Fidler, 'Was Stuxnet an Act of War? Decoding a Cyberattack', in 9 IEEE *Security and Privacy Magazine* (2011) 4, pp.56-59. See also K. Ziolkowski, 'Stuxnet - Legal Considerations', in 25 *Humanitäres Völkerrecht – Informationsschriften /Journal of International Law of Peace and Armed Conflict* (2012), pp.139-147 at pp.146-7, where she discusses whether Stuxnet constituted economic coercion or a violation of the non-intervention principle (the former falls within the latter in my view) and concludes that it is questionable whether the 'Stuxnet' operation breached the principle. With respect, I disagree with her on that point, for the reasons given above. Ms Ziolkowski reaches her conclusion largely on the basis of her reading of the 1986 *Nicaragua* decision of the ICJ where, in paras.244-45, the Court rejected Nicaragua's claim of breach of the non-intervention principle by the US as a consequence of certain economic measures imposed by the US Government (cutting off of economic assistance, reduction of import quota on sugar and a trade embargo). I fail to see that this proves that Stuxnet did not qualify as a form of intervention, since there is little if any similarity between the economic measures ruled upon by the Court in *Nicaragua* and the insertion of a specific type of computer virus into the Iranian nuclear centrifuges reportedly resulting in some degree of physical damage to them. The economic measures imposed by the US Government ruled upon in *Nicaragua* were largely acts of retorsion (cutting off aid, reduction in import quotas) which did not violate any legal obligation, while a selective trade embargo, although potentially illegal, presumably was not seen by the Court as rising to the necessary level of coercion to constitute intervention, even if it caused some economic damage and expressed disapproval of Nicaraguan policies. In contrast, Stuxnet was designed not to cause economic harm or express disapproval, but to prevent or retard a chosen policy of the Iranian Government to allegedly pursue nuclear research for peaceful purposes. In my argument above, I give reasons why I think there are potentially cogent reasons for reaching the conclusion that Iran is acting in breach of the NPT treaty regime and that Stuxnet may qualify as a countermeasure, which may or may not be legal. The essential point for this discussion, however, is that it was a coercive measure designed to prevent a State from carrying out a chosen policy and, since it almost certainly was conducted at the State-to-State level, would *prima facie* qualify as a form of intervention, albeit one which is potentially justifiable.

on the Non-Proliferation of Nuclear Weapons regime to which it is a party,[37] and Iran has undeniably systematically refused to cooperate, or has prevaricated in response to many diplomatic efforts to attempt to induce it to comply. As such, the 'Stuxnet' operation could arguably constitute a countermeasure, which may or may not be lawful, depending on how one assesses the availability of feasible alternatives and the impact of the measure in relation to the threat posed by an Iranian nuclear breakout.

4.2 Available and Possible Remedies in Response to Cyber Intervention

Aside from the obvious step of improving the security of governmental and other critical cyber systems, and the very limited possibilities of effectively prosecuting foreign State agents who might be implicated in illegal acts of cyber interference for the reasons set out previously, there are a number of other possible options for response to (attempted) cyber intervention, based on those mentioned above in more general terms, which may be available to a State which is the target of cyber intervention.

The most important of these include measures of active cyber defence which, depending on the circumstances, could either qualify as measures of retorsion, or as countermeasures. Such active cyber defence measures could include measures aimed at misleading a prospective intervening party by providing it with bogus or useless information or otherwise diverting cyber break-ins from their intended targets. They could rise to the level of 'hacking back' to the source of the cyber intervention and temporarily or permanently disabling, damaging or destroying the intervening party's systems which were being used to achieve or attempt a form of cyber interference rising to the level of coercive cyber intervention. In the case of causing significant or long-term damage to the intervening State's systems, the measure would constitute a countermeasure, which could be lawful if the conditions for taking a countermeasure, as set out above, were complied with. In cases where the remedial action simply misled or diverted an attempted cyber break-in amounting to intervention, or caused a temporary disabling of the intervening State's system being used for the (attempted) intervention, no violation of international law would occur and the measure would qualify as an act of retorsion, analogous to the interception of a foreign State aircraft engaging in unauthorised penetration of national airspace or the forcible expulsion of foreign submarines engaged in non-innocent passage in territorial waters. However, even if lawful, it would be imperative to restrict such remedial action to State (law enforcement) agencies and agents (whether civilian or military) who were acting under governmental authority and were subject to effective oversight and accountability procedures to prevent 'vigilantism' and unnecessary escalation.[38]

---

37 *Treaty on the Non- Proliferation of Nuclear Weapons* of 1 July 1968, 729 U.N.T.S. 161, entered into force on 5 March 1970.

38 For a recent discussion of the dangers related to active cyber defence, in particular, allowing private corporations or State licensed security firms to engage in 'hacking-back' in response to unauthorised break-ins and theft of data, see 'Business and cyber-crime: Firewalls and Firefights', *The Economist* (10-16 August 2013), pp.47-48.

Such cyber countermeasures and forms of retorsion could, and probably should, have a place alongside more traditional forms of retorsion and countermeasures and, provided they fully complied with all the conditions under international law for the taking of such remedial measures, would be a lawful response to attempts by a foreign State to engage in illegal cyber interference and intervention. There is no legal reason why a State should be denied such a possible response to illegal activities aimed at undermining its authority or preventing it from engaging in activities and pursuing policies which it is entitled to do under international law. It is unrealistic to expect a State to simply stand by and allow its authority or lawful activities to be undermined or coercively prevented from going about its lawful business, and it is equally undesirable to needlessly escalate such remedial action into measures which would be disproportionate or unlawful in relation to the illegal interference or intervention by the other party.

However, it is equally important to recall that, as stated previously, such remedies are no 'cure-all' and that the taking of remedial action in the form of either lawful measures of retorsion, or countermeasures, is not always feasible, nor always the best or only possible response to unfriendly or illegal activity by a foreign State, due to the possible escalatory effects they could have, and the lack of certainty in many cases as to who or what is the responsible party. If this is true in the physical domain, there is no reason why this should be any different, in principle, in the cyber context. Consequently, such remedial action should be used judiciously and only when it is both clear who is the responsible party and when it is likely to be an effective response which does not cause more problems than it is designed to counteract. Moreover, such measures should be an exclusive State prerogative and activity, subject to clear oversight and accountability to avoid abuse and vigilante behaviour by private individuals.

5. Some Concluding Remarks

In the introduction, a number of questions were posed relating to the nature and content of the non-intervention principle under international law, both in a general sense and how this may translate into the cyber context. It was determined that the principle of non-intervention is related to State sovereignty and prohibits 'dictatorial' or coercive activity which is aimed at undermining a State or overthrowing its government, or otherwise is intended to, or has the effect of, coercively preventing or forcing a State to do something which it is entitled to do or abstain from doing under international law. It includes military intervention, but is wider than simply restating the prohibition of the use of force. It is a principle which is exclusively aimed at States and from which States draw an entitlement to order their domestic affairs and pursue policies which are not otherwise regulated by or which are prohibited under international law. Since intervention is unlawful, it engages the responsibility of the State which conducts it, to the extent the acts concerned can be attributed to a particular State or States. These rules are, by and large, set out in the *Draft Articles on Responsibility of States*

for Internationally Wrongful Acts which were drawn up by the ILC. There are several possible remedies available under international law to the State which is the target of unlawful intervention. These include, under limited circumstances, the exercise of criminal jurisdiction over State agents involved in acts of unlawful intervention, provided there is sufficient evidence to enable prosecution, the persons are present on State territory and they do not benefit from diplomatic or sovereign immunity and are therefore subject to prosecution. In addition, there are the classical self-help measures of retorsion and reprisal (countermeasures), which can, subject to the conditions posed under international law for their exercise, be employed in response to (attempted) acts of interference amounting to intervention. It was determined that this general legal framework applies to coercive cyber activity which is intended to have, or actually has, the same basic effects as intervention in the physical domain and that there are various forms of cyber activity which could potentially constitute such coercive intervention. Finally, it was determined that the same basic remedies can be applied in the cyber context to such coercive cyber intervention, subject to the same legal conditions which apply to the taking of remedial action in the physical domain. It was argued that certain types of 'active cyber defence' could qualify as either retorsion or countermeasures, depending upon the circumstances, and that they could potentially play a useful role in countering such intervention, albeit one which should be used judiciously, and which will not necessarily always be feasible or effective.

In closing, it is important to re-emphasise that the principle of non-intervention is well established and has a specific place under international law. It may sound rather antiquated in the present world of instant cyber communication and global interdependence to devote attention to the right of States to non-interference in their domestic affairs, but as long as States remain the principal actors in the international system, it will remain a pertinent and relevant principle of international law and relations. States and their citizens have a right to order their affairs according to their laws and customs, just as individuals do. Nevertheless, it is not, nor has it ever been, unconditional and there are many areas of activity which are the legitimate concern of the international community. Likewise, intervention should not be confused with other forms of cyber activity, either illegal or legal, and should be properly distinguished from acts which, while intrusive, do not constitute intervention. Nevertheless, since it is possible to engage in coercive cyber activity which constitutes intervention, it is undoubtedly a phenomenon which is here to stay, even if its occurrence is likely to be rather limited. As such, it is reasonable to look at ways in which States may lawfully react to such coercive interference. Hopefully, this chapter will provide a useful contribution to the discussion of these possibilities and their limitations.

Dinah PoKempner

Cyberspace and State Obligations in the Area of Human Rights

1. Cyber Communications as a Human Rights Accelerator

At one time the internet was often described in utopian terms. It would liberate all knowledge, return power to the hands of the people, make government either redundant or accountable and usher in an era of equality and the realisation of democracy and human rights. These heady days are largely past, and a grimmer appreciation of the threats facilitated by cyberspace and the attacks possible against a secure and free use of cyberspace is prevalent. Private and State actors vie to control and monitor electronic communications, posing serious challenges to the idealistic view of a global commons. Yet, in terms of the realisation of democratic and human rights, a core optimism is still justified because the internet has, in fact, opened the floodgates of information to more people around the world, has empowered many who were previously powerless, and has increased pressure on governments to be more transparent and accountable than ever before.

The centrality of the internet, and electronic communications more generally, to human well-being in the twenty-first century is hard to overstate. Commerce, finance, infrastructure management, education, politics, labour relations, journalism, law; these and most other key economic, intellectual and cultural institutions of contemporary human society have moved online. While it is possible for an individual to live a happy life unconnected to the internet, there are few modern societies where that individual's welfare is unaffected by the existence of a background cyber world supporting his or her enjoyment of rights. Conversely, attacks on cyberspace can jeopardise not just the gains in human welfare brought about by digital online social relations, but might even place societies in a worse position than before this reliance on the internet revolution.

This reality underpins the human rights dimension of cyberspace. Access to cyberspace, and freedom to communicate and receive information online, are enabling, lynchpin freedoms, important not just in themselves, but as necessary conditions for the realisation of a much wider set of human rights. Cyberspace technologies have not only placed the realisation of many fundamental rights within the reach of many more people, but the exercise of these rights is increasingly dependent on the protection and safeguarding of the internet and, in particular, the internet as a domain of freedom.

The amplification of common civil and political rights through cyber communications is obvious. Traditional media, such as newspapers, university conferences, libraries and radio broadcasts, through which freedom of information and expression in any given

society are realised, are rapidly moving online. However, even as these enterprises stake their place on the web, new forms of public reporting, information sharing and creative collaboration are developing: bloggers and tweeters, interactive wiki sites, chat rooms and mash-ups, to name a few. These new fora and speakers deserve the same protection as the more traditional editorial columns, podia and journalists, but are sometimes excluded from hard-won protections for the press. Rights that rely on the ability to associate with others of similar views translate clearly to online activity of similar character deserving similar legal protections. Registration and voting traditionally happened in community halls, but now can happen online; one might go to the local coffee house for jam sessions, poetry slams or performance art, or online for crowd-sourced operas, novels and paintings.

Economic, social and cultural rights are also set to reap great benefits from online communications. Many development programmes are now centred on digital literacy and the facilitation of access to online resources in education, cultural heritage, health, weather, market conditions and other types of information that is essential to protecting and advancing basic rights. Although the vast majority of online content is in English, this picture is changing rapidly, and new technologies for translation are narrowing the global inequities known as the 'digital divide'. Projects that focus on text or mobile phone-based applications can be accessible to even the poorest communities, and create new forms of community organising that can overcome barriers in distance and transportation.

This growing reliance of societies on cyberspace as a means of advancing rights has led the United Nations (UN) Special Rapporteur Frank La Rue, in his May 2011 report, to call for internet access to be maintained even in times of political unrest, and for the penalty of cutting off internet access to any individual to be considered presumptively disproportionate in view of the harm to the rights of expression and information.[1] In the same report, he concluded that since 'the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States.'[2]

Some of the elements which have made cyberspace so uniquely valuable to the realisation of human rights include: the low-cost accessibility of vast amounts of content across borders; the interactivity of version 2.0 platforms; the ability to link to, and host, vast amounts of third party content from every corner of the globe; and the ability *even when networking with others* to protect personal privacy, either through anonymous

1 Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (UNGA, Human Rights Council 17th session, UNGA Doc. A HRC/17/27, 16 May 2011) paras 78, 79 [hereinafter Report of the Special Rapporteur 2011].

2 Ibid, para 85.

access and communication, or through the withholding of personal information from collection, retention or transfer by others.

Special attention should be given to the networking power of cyberspace as a rights accelerator. Social media sites are both proliferating and concentrating; they enable not only solidarity and new communities, but also facilitate the aggregation of information through crowd-sourcing, which can give many potential actors a broad perspective on crises in real time. 'Ushahidi', a crowd-sourcing platform, has been applied to mapping locations of Haitian earthquake victims to aid rescuers, plotting real-time sexual assaults against the Cairo city grid to aid women and, most recently, tallying disease and morbidity data throughout Syria. Market giants such as Facebook, Twitter and Google are fundamentally changing how politics, propaganda, and even revolutions are conducted, throwing the policies of these corporations into the spotlight, as they often have as much or more influence on the rights they facilitate as government regulation does.

As a medium of global information exchange and organisation, cyberspace enables activists not only to raise awareness of rights and the rule of law, but to hold government accountable. The revolution in Egypt illuminated many of these attributes in action. Wael Ghonem, a young Egyptian outreach and marketing manager for Google, based in Dubai, created a Facebook page to publicise a typical but outrageous act of impunity in Alexandria: the brutal murder of Khaled Said, another young professional dragged out of an internet cafe by police who assaulted him for posting on YouTube a video of officers divvying up a haul of confiscated marijuana. Ghonem's site, featuring mobile phone pictures of Said's crushed face in the morgue, attracted hundreds of thousands of followers, and became a vector for channelling outrage and protest action against corrupt, abusive and undemocratic governance.[3] Ghonem, who used a proxy to enable personal anonymity as to his management of the site (a difficult issue given Facebook's 'real name' policy), was identified to the Egyptian police and arrested; on release, his emotional television interview galvanised yet more support for the street protests that had begun in the meantime. The information, responses, and gathering solidarity of the network percolated through the universities, streets and mosques of Egypt, and eventually led to the overthrow of the government and the verdict against former President Mubarak. Yet Ghonem disclaimed a leading role. In his words:

> Our revolution is like Wikipedia, okay? Everyone is contributing content, [but] you don't know the names of the people contributing the content. This is exactly what happened. Revolution 2.0 in Egypt was exactly the same. Everyone

[3] This case has been both touted and disclaimed as an outstanding example of social action in the internet age. For various accounts, see Gordon Crovitz, 'Egypt's Revolution by Social Media,' *The Wall Street Journal* (New York, 13 February 2011); Malcolm Gladwell, 'Does Egypt Need Twitter?' *The New Yorker* (New York, 2 February 2011); Navid Hassanpour, 'Media Disruption Exacerbates Revolutionary Unrest: Evidence from Mubarak's Natural Experiment' (2011), APSA 2011 Annual Meeting Paper.

> contributing small pieces, bits and pieces. We drew this whole picture of a revolution. And no one is the hero in that picture.[4]

The particular qualities that make the internet a powerful instrument for grass-roots organisation have conversely prompted States that fear popular challenge to try and control social media platforms. China's reaction to the Arab Spring has included not only careful attention to its blogosphere and the issues that draw virtual crowds, but also a crackdown on popular critical bloggers, the deployment of legions of State-paid 'netizens' to shape popular comment, and new laws to control social media. Other policies employed by States that would prefer to restrain rights and avoid the strong rule of law include: blocking and filtering content; restricting access to content; banning strong encryption or requiring that government always gets a 'backdoor' key; enforcing 'real name' policies; imposing full and immediate liability on intermediary hosts to coerce their collaboration in censorship, and creating new speech crimes or enhanced penalties for existing crimes when committed through cyber means. In such societies, one also sees extra-legal countermeasures on the part of the State or its agents, such as employing intrusive electronic surveillance, impersonation, denial of service attacks, and other types of online and physical attacks and interference directed against those deemed cyber dissidents.

Human security and human rights are also under threat from private (and sometimes State) actors who exploit the wealth of information, the speed, the global reach and networking powers of cyber communications for either personal reasons such as gain or animus, or for political or national security reasons. In the former category we would recognise many ordinary offences in civil and criminal law, from copyright infringement, data theft, fraud, defamation or intrusion. In the latter, we might find direct action protests, terrorism, espionage and even attacks, whether committed by State or non-State actors, which may activate the application of international humanitarian law (IHL). A wide variety of legal regimes may apply to such malevolent acts, which are often conducted across borders, complicating jurisdiction and enforcement actions.

Attacks that threaten online communications and networks, and the rights these enable, will activate a State's responsibility to protect. At the same time, the State is constrained by international law in its response, under principles of necessity and proportionality which are common to both human rights and humanitarian law. These legal regimes apply to actions in both the physical and virtual worlds, as discussed in the following section.

---

4 The statement was made on the 13 February 2011 broadcast of the television show '60 Minutes'. Nancy Scola, 'Ghonim: "Our revolution is like Wikipedia,"" *TechPresident* (14 February 2011), available at http://techpresident.com/blog-entry/ghonim-our-revolution-wikipedia.

2. The General Application of Human Rights Law to Cyber Activities

The proposition that human rights apply to digital events, online media and cyber technologies is also well-accepted at this point. The basic guarantee of freedom to receive and impart information is explicitly framed in international law to apply without qualification as to borders or media used.[5] With regard to other rights implicated in online expression, the fact that a given activity is entitled to some human rights consideration generally does not depend on the medium or locus of an activity, though these issues may have a bearing on how much, or what type of, protection is due. For example, religious practice merits consideration as a human right even if not situated in a church or expressed through reading prayers; political association may be effectuated through broadsides or bullhorns, and education is no less a right should it take place off or on a campus. Similarly, all these activities retain protection as rights even when taking place online. On 5 July 2012, the UN Human Rights Council adopted by consensus a resolution that not only recognised the value of the internet to human rights, but explicitly affirmed:

> [T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[6]

The obligations of human rights law derive from sources such as the Universal Declaration of Human Rights (UDHR), which is increasingly accepted as articulating norms of customary international law, as well as from international treaties such as the *International Covenant on Civil and Political Rights* (ICCPR), and regional treaties, including the European and American conventions on human rights. A large body of authoritative and influential sources interpret or elaborate these, including notably the jurisprudence of the European Court of Human Rights, the General Comments of the Human Rights Committee (the treaty body of independent experts that monitors the implementation of the ICCPR), findings and reports of UN Special Rapporteurs, UN General Assembly resolutions and important statements of non-official expert bodies,

---

5 See, e.g., Article 19 of the Universal Declaration of Human Rights [hereinafter UDHR] (right to 'receive and impart information and ideas through any media and regardless of frontiers.'); Article 19(2) of the *International Covenant for Civil and Political Rights*, UNGA Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, (UNGA Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force 23 March 1976) [hereinafter ICCPR] ('regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.'); Article 10(1) of the *European Convention on Human Rights* [hereinafter ECHR] ('regardless of frontiers'); Article 13(1) of the *American Convention on Human Rights* [hereinafter ACHR] ('regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice').

6 UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet (UN Human Rights Council 20th session, UN Doc. A/HRC/20/L.13, 29 June 2012).

such as the Johannesburg Principles on National Security,[7] the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights[8] (or, even more recently, evolving civil society statements that are still gathering comments and support, such as the draft *Charter of Human Rights and Principles on the Internet*[9]). Municipal law, including constitutional law and judicial decisions, provide additional models and sources for interpretation, development and application of international standards.

Rights, such as freedom of expression and information, privacy, and freedom of association are subject to some normal limitations under international law. Restrictions that are acceptable under the ICCPR and regional treaty law must be:

- contained in law that is written, with accessible rules of sufficient clarity and specificity to permit the public to foresee their reasonable application to conduct and not conferring excessive executive discretion;
- protecting a legitimate interest in a democratic society, such as protection of the rights of others, public safety or national security, but not simply avoiding embarrassment of the government, concealing wrongdoing or entrenching a particular ideology or party;
- a 'necessary' and 'proportionate' means of achieving that aim, that is, the least restrictive means of securing the interest to be protected, and
- susceptible to judicial review and remedy.[10]

Additionally, State obligations with respect to these rights extend to protecting persons against violations by other private actors (known as 'indirect' or 'horizontal' effects of human rights law); extending protection to all persons within the territory or subject to the jurisdiction or effective control of the State, and avoiding invidious discrimination in the enforcement and respect of rights.

---

7 The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (UN Doc. E/CN.4/1996/39, November 1996), available at http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf.

8 UN Commission on Human Rights, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, (UN Doc. E/CN.4/1985/4, Annex, 28 September 1984), available at http://www1.umn.edu/humanrts/instree/siracusaprinciples.html.

9 Charter of Human Rights Principles and the Internet, Version 1.1 Draft (2012), available at http://internetrightsandprinciples.org/site/wp-content/uploads/2012/12/Charter-on-Human-Rights-and-Principles-on-the-Internet-Version-1-1-Draft.pdf.

10 Ian Brown and Douwe Korff, *Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online* (see particularly sources cited in notes 17 and 18) (Global Network Initiative, July 2012), available at https://globalnetworkinitiative.org/content/digital-freedoms-international-law; see also Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (UNGA, Human Rights Council twenty-third session, UN GA Doc. A/HRC/23/40, 13 April 2013) [hereinafter Report of the Special Rapporteur 2013] paras 28, 29 and also Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights 1985 (n 8) and the Johannesburg Principles on National Security, Freedom of Expression and Access to Information 1995 (n 7).

Turning for a moment to IHL, there is considerable agreement that its principles apply to cyber weapons and cyber warfare, as evidenced by an emergent body of scholarship on this issue.[11] New weapons are typically tested against IHL standards and, indeed, to claim that cyber war methods are not susceptible to the fundamental principles of distinction and proportionality would be to throw into doubt their legality. However, it is important to recognise that the application of either *jus in bello* or *jus ad bellum* would be unlikely in the vast majority of cases of malevolent cyber events. There are many reasons, among them that war (as a context for evaluating any given attack) is less common than peace, that the severe effects of the sort that would elevate a hostile cyber event to the requisite level to justify resort to force in self-defence or which would constitute an 'attack' in IHL terms, are uncommon, and obtaining a sufficient degree of attribution to justify a resort to force, or calculate proportionality in any given instance may be complex or elusive. The overwhelming majority of malevolent cyber events affecting any given society are more accurately characterised as crimes, torts, espionage or human rights violations rather than as acts of war. This makes it particularly important to consider the normal peacetime framework of law with respect to the State's obligation to ensure rights.[12]

However, in any given case of armed conflict, it is also an increasingly dominant view that international human rights law (IHRL) continues to apply, except where displaced in particular matters by the *lex specialis* of IHL.[13] Armed conflict is also considered a traditional situation where derogation, or restrictions on rights beyond those normally permitted, may be justified. Yet restrictions in case of war or other public emergency threatening the life of the nation are also narrow in scope. They must firstly be measures 'strictly required by exigencies of the situation' including in scope and temporal duration.[14] They must be 'officially proclaimed' and specifically notified to other parties

11 See, e.g., Michael N. Schmitt (gen. ed.), *Tallinn Manual on the International Law Applicable to Cyberwarfare* (Cambridge 2013), available at http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381.

12 See Article 2(1) of the ICCPR.

13 See UN Human Rights Committee (HRC), *General Comment No. 31 [80] Nature of the General Legal Obligation Imposed on States Parties to the Covenant* (ICCPR document CCPR/C/21/Rev.1/Add.13, 26 March 2004) para 11: 'As implied in General Comment 29 on States of Emergencies, adopted on 24 July 2001, reproduced in Annual Report for 2001, A/56/40, Annex VI, paragraph 3, […] the Covenant applies also in situations of armed conflict to which the rules of international humanitarian law are applicable. While, in respect of certain Covenant rights, more specific rules of international humanitarian law may be specially relevant for the purposes of the interpretation of Covenant rights, both spheres of law are complementary, not mutually exclusive.' It should be noted that the United States (US) has voiced its opposition to this view, aware however that it is the dominant view of the international community. This chapter does not purport to examine issues of human rights in the context of armed conflict or where areas of potential inconsistency between the two regimes may exist because, as noted in the text, these will perforce be unusual situations. However, it is the author's belief that in fact, many areas of human rights law, such as criminal procedure guarantees, non-discrimination principles, etc., would remain relevant in any such analysis.

14 Article 4(1) of the ICCPR; Article 15(1) of the ECHR.

to the ICCPR.[15] Finally, they must not involve discrimination solely on the ground of 'race, color, sex, language, religion or social origin.'[16]

In addition to the norm against invidious discrimination, many other general principles of law come into play with regard to restrictions on rights in either the IHRL or the IHL context. So, for example, foreseeable harm to bystanders or civilians must be calculated in either the context of law enforcement or military attack to determine whether the State's action could be justified as proportional or necessary under the relevant standards. Criminal penalties cannot be imposed where the attribution of an act is in doubt or indeterminable, collective punishment cannot be used, and *ex post facto* laws are impermissible. Laws, even when promulgated to address a genuine emergency, must be sufficiently precise to give notice of the circumstances to which they apply, must address a genuine public interest and must be fully justiciable, including with regard to their substantive validity, and not merely procedural or formal validity in their application to any given case.

While cyberspace is hardly *terra nullius* for the purpose of international law, the application of existing laws do present problems given the trans-border nature of many actions online. National law regulates much online activity, most robustly (but not exclusively) when the relevant acts take place within a national territory. The ordinary laws of tort, intellectual property, and a good deal of criminal law connected to speech acts apply to online behaviour. Mutual legal assistance treaties and substantive treaties on issues of cyber crime and data protection address some of the complexities of regulation across borders, but are not always effective at either addressing wrongful acts or protecting human rights. With both the general principles and the complexities of enforcement in mind, we turn to specific issues engaging human rights and cyberspace.

3. Positive Obligations to Provide Access to Cyberspace

Access to information is not only a right in itself, but is also a necessary condition of the fulfilment of many others. While international covenants do not contain an explicit right to water, for example, it is common to speak of access to water as a 'right' insofar as it is well understood it is indispensable to fundamental rights such as life, health, food, and the right to a living.[17] In a similar fashion, access to online information is increasingly essential to enjoyment of nearly every other right, whether civil, political, economic, social or cultural. The Human Rights Committee, in its new General Comment 34 on

15 Article 4(1) of the ICCPR.

16 Ibid.

17 See, e.g., World Health Organization, 'The Right to Water' (Geneva, 2003), available at http://www2.ohchr.org/english/issues/water/docs/Right_to_Water.pdf, and Office of the High Commissioner for Human Rights issue page on the right to water, including information on the Special Rapporteur on the human right to safe drinking water and sanitation, who assumed her mandate in 2008, available at http://www.ohchr.org/EN/Issues/WaterAndSanitation/SRWater/Pages/SRWaterIndex.aspx.

Freedom of Opinion and Expression, noted the importance of States ensuring both universal access to, and the independence of, new media such as the internet.[18]

While acknowledging that 'access to the internet' is not yet recognised formally as a right, Special Rapporteur La Rue also urged States to 'make the Internet widely available, accessible and affordable to all' given that it has become 'an indispensable tool for full participation in political, cultural, social and economic life.'[19] To that end, he highlighted the need to facilitate access to marginalised groups, including women and the disabled, and the importance of using the internet to promote education and materials in minority languages.

4. The Criminalisation and Punishment of Cyber Offences

Another positive obligation of States under IHRL is to protect those persons within the State's territory and control from others who would violate their rights.[20] In practice, much malicious activity in cyberspace traduces criminal law of either a municipal or international character. Cyber crime agreements and laws are proliferating, and comprise a wide variety of harmful acts, such as fraud and password trafficking, data theft, online child pornography, harassment, gambling, hacking, denial of service attacks and malicious destruction. Typical grounds for State failure to ensure rights include inadequate legislation or means of enforcement; an inadequate commitment to rule of law, transparency, and accountability even where legislation exists; procedural violations in the application and enforcement of law, and the outlawing or punishing of activities that should enjoy substantive human rights protection.

Where inadequate legislation is a root cause, the issue is often a failure to translate norms developed in the physical world to the virtual world. For example, when a hacker intrudes and copies passwords or valuable data, a conventional statute on 'theft' might not cover an action that does not deprive the owner of the information, but merely spreads it to others.[21] In a recent survey conducted by the UN Office on Drugs and Crime, many less developed countries reported what they perceived to be an inadequate coverage of substantive and procedural criminal law to cyber crimes.[22]

The substantive incompatibility of cyber crime law with human rights law is yet another problem. In some countries, laws punish speech and associations that are unambiguously protected by IHRL, such as peaceful political dissent or criticism of the government.

---

18 UN HCR, *General Comment No. 34 – Freedom of opinion and expression* (ICCPR document CCPR/C/GC/34, 12 September 2011) para 15.

19 Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (UN GA Doc. A/66/290, 10 August 2011) para 63.

20 See Article 2(1) of the ICCPR, and 'General Comment No. 31 [80]' (n 13) para 8.

21 UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (February 2013) 52, available at http://www.unodc.org/documents/commissions/CCPCJ_session22/13-80699_Ebook_2013_study_CRP5.pdf.

22 Ibid xvii and Chapter 4 for detailed results.

In the area of transnational crime and enforcement, different national laws and legal traditions may give varying interpretation to human rights obligations, with one State criminalising activity that is considered protected expression under human rights law, either by an international adjudicator or the legal system of another (examples could include instances of hate speech, 'glorification' of terrorism, criminal defamation or insult). The incompatibility of a prosecuting State's law with constitutional or international human rights obligations of another State may defeat criminal cooperation and enforcement efforts. In this regard, the dual criminality provisions of the Council of Europe's *Convention on Cybercrime*, which require enforcement cooperation from a State party with respect to acts that do not constitute crimes under its own laws, have raised concerns.[23]

Laws that require filtering or blocking access to content that might validly be susceptible to limitation under human rights law can often serve as dragnets or excuses to target more broadly. Special Rapporteur La Rue expressed strong concern at State practice in blocking entire websites, social media platforms, or topics (such as 'human rights' or 'democracy') as well as timed and targeted blocks to discourage political debate at sensitive times, such as the lead-up to elections, noting that blocking lists are generally kept secret, making assessing or challenging the aim of the restriction difficult or impossible.[24] Although restriction of child pornography is one of the few categorical content restrictions that generally can be justified under Article 19 of the ICCPR, examples abound of child pornography filters catching websites of organisations that campaign against child pornography, or other, entirely benign, sites. Moreover, there is no evidence that blocking has actually lessened the exploitation of children through trafficking or pornography, although it does remove the issue from the view of a public that might demand more effective action.[25]

Just as criminalisation of content, while sometimes justified or required under IHRL,[26] can easily slip into the zone of violation of rights, so can intellectual property enforcement on the web. Enforcement of laws that appear either positive or neutral in terms of human rights can also be misused to persecute or discriminate. For example, in 2010, Russian security services carried out dozens of raids against activist groups

---

23 But see Susan Brenner, 'Cybercrime treaty: criticisms' *Cyb3rcrim3* (16 August 2006), available at http://cyb3rcrim3.blogspot.com/2006/08/cybercrime-treaty-criticisms.html (contending that Article 15 of the treaty allows the US to 'import our Bill of Rights' and that Article 24 would bar extradition except where double criminality exists).

24 Report of the Special Rapporteur 2011 (n 1) paras 29, 30 and 31.

25 Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic 2012) 96-97.

26 In some instances, IHRL requires prosecution of speech crimes, such as incitement to genocide (Article 3(d) of the *Convention on the Prevention and Punishment of the Crime of Genocide*, 78 U.N.T.S. 277, entered into force Jan. 12, 1951, 'direct and public incitement to commit genocide' shall be 'punishable') in others, specific violations must be 'prohibited by law' which is often, but not necessarily, interpreted to mean criminalisation (e.g., Article 20 of the ICCPR; hate speech and propaganda for war).

for allegedly using pirated Microsoft software. When this was revealed by *The New York Times*, it prompted Microsoft to change its enforcement policy to guard against manipulation against political advocacy.[27] Key objections to the doomed US *Stop Online Piracy Act* (SOPA) were overreaching provisions that would have allowed prior restraint of allegedly infringing sites before the opportunity of an adversarial hearing, ambitious extraterritorial application, and the destruction of the domain name system's global uniformity by court fiat.[28] The *Anti-Counterfeiting Trade Agreement* has been similarly criticised for overreaching on intellectual property enforcement to the detriment of public interests in internet service provider (ISP) protection, freedom of information, and other public goods such as affordable medicine.[29] In 2013, the respected human rights group, Article 19, put forward principles of freedom of expression and copyright derived from IHRL to remind policymakers that denial of access to the internet and criminal penalties are always disproportionate sanctions for copyright infringement, that access to remedy for infringement should always require proof of copyright, and that prior restraint be subject to adversarial challenge.[30]

Finally, procedural aspects of cyber crime laws may raise human rights concerns, particularly with regard to the preservation and accessing of evidence where privacy rights are threatened by unrestrained or inadequately supervised powers of search and surveillance. Securing evidence across borders is often critical to the effective investigation and suppression of cyber crime. However, national laws on search and seizure and data protection vary widely, as do consequences under national law in a trial when the government is found in breach of such legal strictures. The Council of Europe's *Convention on Cybercrime*, which is the oldest and foremost international treaty on this subject, has been criticised for requiring governments to assume broader authority to search and seize various types of data in real time, and impose gag orders on ISPs subject to such orders, without specifying oversight of such powers or minimum standards for the respect of privacy other than by reference to the very broad guarantees of general IHRL, such as the ICCPR and the *European Convention on the Protection of Human Rights and Fundamental Freedoms* (ECHR).[31] In some jurisdictions, the standards for requiring production of digital information or 'backdoor' searches are

27 MacKinnon (n 25) 107.

28 See, e.g., Letter to Lamar Smith, Chairman, Committee on the Judiciary, 15 November 2011, available at https://www.cdt.org/files/pdfs/Public_Interest_SOPA_Letter%20(1).pdf. A catalogue of documents setting out objections to SOPA from human rights organisations and hundreds of others is available at https://www.cdt.org/report/list-organizations-and-individuals-opposing-sopa.

29 See, e.g., Alexander Furnas, 'Why an international trade agreement could be as bad as SOPA,' *The Atlantic* (6 February 2012), available at http://www.theatlantic.com/technology/archive/2012/02/why-an-international-trade-agreement-could-be-as-bad-as-sopa/252552/.

30 Article 19, *The Right to Share: Principles on Freedom of Expression and Copyright in the Digital Age* (see principles 8, 12 and 10) (London: 2013), available at http://www.article19.org/data/files/medialibrary/3716/13-04-23-right-to-share-EN.pdf; see also Report of the Special Rapporteur 2011 (n 1) pars 49 and 50.

31 See Article 15(1) of the *Convention on Cybercrime* (3 November 2001); see also Nancy E. Marion, 'The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation' *International Journal of Cyber*

lower than the court-approved warrants required for physical searches and intrusions.[32] Many corporate intermediaries are only too willing to comply, mainly because they have no obligation or incentive to challenge, much less request, governments to be transparent about the demands they impose. Where national security is invoked, we can expect government resistance to transparency.

5. Data Protection and Data Retention

Both data protection and data retention strongly engage the right to privacy, and have been controversial areas in regulating cyber activity. The right to privacy is neither unconditional nor non-derogable. As qualified in the UDHR, interference must not be 'arbitrary'[33] and, in the terms of the ICCPR, it may not be 'arbitrary' nor 'unlawful.'[34] The ECHR states it somewhat differently, in that interference with the right may not be 'except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[35] There is some scholarly discussion as to whether the European formulation of the right or the international formulation is more subject to limitation.[36] In light of the limited jurisprudence of the Human Rights Committee, commentators tend to refer to the criteria in play in the cases of the European Court of Human Rights, namely whether an invasion of privacy is to safeguard a legitimate State interest (and consistent with respect for other human rights generally), whether it is necessary as well as proportional in scope and duration to that aim, and whether the law is sufficiently specific and accessible to give notice to people as to the extent of the restrictions on privacy it would foreseeably authorise. These appear to be generally consistent with the Human Rights Committee's interpretation of Article 17 of the ICCPR.[37]

Criminology (Vol. 4, Issue 1&2, January-July 2010 & July-December 2010) 704-795, available at http://www.cybercrimejournal.com/marion2010ijcc.pdf.

32 The US *Electronic Communications Privacy Act*, for example, allows law enforcement authorities in the US to demand electronic data without a warrant if was stored for more than 180 days.

33 Article 12 of the UDHR.

34 Article 17(2) of the ICCPR.

35 Article 8(2) of the ECHR.

36 See, e.g., Manfred Nowak, *U.N. Covenant on Civil and Political Rights CCPR Commentary* (Kehl am Rhein, Strasborg, and Arlington, VA, N.P. Engle 1993) 290-294.

37 See HRC, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (8 April 1988), available at http://www.refworld.org/docid/453883f922.html, para 4 ('The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.'), para 7 (only private information 'essential in the interests of society as understood under the Covenant' may be compelled), and para 8 ('legislation must specify in detail the precise circumstances in which such interferences may be permitted.').

Data protection laws typically give persons control over who may access their personal data, what it may be used for, how it should be stored, and for how long. Their importance and spread has grown in response to the aggregation and retention of personal information through the cyber activities of both State and private actors. Such information can take not only the form of names and email metadata, but also visual, medical, DNA, historical, financial and locational data, collected through numerous agencies. Special Rapporteur Frank La Rue has noted insufficient or inadequate data protection laws in many countries, a situation that is of concern given the increasing use of multi-locational cloud computing services and the tendency of States to request or require companies to hand over data on their users.[38]

Article 17(2) of the ICCPR provides that '[e]veryone has the right to the protection of the law' against arbitrary or unlawful interference with privacy, family, home or correspondence.[39] The Human Rights Committee, as long ago as 1988, interpreted this provision as requiring for every person:

> the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[40]

As this passage suggests, data retention (or stated differently, the right to not have one's personal data retained) is the other face of data protection. The European Court of Human Rights has held that the indefinite retention of biodata such as fingerprints, cell samples and DNA profiles from persons suspected of, but not convicted of, crimes was an intrusion into privacy that was disproportionate to the public interest which was sought to be protected.[41] However, it also held there was no disproportion in the inclusion of persons in a national sex offender database who had been convicted of rape of minors when the period of data conservation was at most 30 years and the data itself was subject to restricted access and a duty of confidentiality.[42] It has also held a violation of privacy where archived personal history information was not subject to judicial control and review,[43] and where personal historical information on the applicants was

38 Report of the Special Rapporteur 2011 (n 1) para 56.

39 Article 17(2) of the ICCPR; see also Article 12 of the UDHR.

40 HRC, CCPR General Comment No. 16 (n 37) para 10.

41 *S. and Marper v. the UK* [2008] ECtHR App Nos. 30562/04; 30566/04, [2008]; *Van der Velden v. The Netherlands* [2006] ECtHR Decision App No 21203/10, (2006); see also *M.K. v. France* [2013] (no. 19522/09), concerning retention of fingerprints of a criminal suspect who was not convicted.

42 *B.B. v. France*, *Gardel v. France* and *M.B. v. France* [2009] ECtHR App Nos. 5335/06, 16428/05, 22115/06. [2009].

43 *Rotaru v. Romania* [2000] ECtHR App No 28341/95, [2000].

withheld by the Swedish Security Police for reasons insufficiently relevant to present national security concerns.[44]

We have yet to see whether the European Court of Human Rights will become more sensitive to data retention issues in the wake of the revelations of bulk data surveillance on the part of the United States (US) government and many European governments. However, the European Parliament is proposing to tighten rules on data transfer and retention with respect to private companies and, in particular, would require US companies to seek permission from European officials before complying with US government demands for private data on Europeans.[45] As the rules would not apply to national intelligence services, it remains to be seen whether popular anger over bulk surveillance programmes will prompt any change in the municipal regulation of European governments' data collection and retention policies.

6. Surveillance and Espionage

The surreptitious monitoring, capturing or copying of online information can be performed by either State or non-State actors, for reasons as diverse as protecting national security, economic advantage or personal malice. While data theft, intrusion, hacking and breach of data protection are typically offences in municipal law, digital surveillance within a jurisdiction by the jurisdiction's own authorities is often much more loosely regulated, with considerable latitude given to State authorities which act for established purposes, such as the protection of national security or law enforcement.

State-sponsored surveillance tends to be discounted as a 'passive' or invisible intrusion, but when conducted on a pervasive scale, it is an activity that can severely harm rights in several dimensions. Firstly, the invasion of privacy occurs at the point of intrusion and capture of material, not only at the point of access or use of information. The inability to direct one's communications to only those who are intended recipients is a serious loss of control over one's identity and autonomy; everyone has experienced the sensation of literally 'being a different person' when in public, as opposed to among intimates. The uncertainty over which communications will be accessed when, and by whom, can also chill the exercise of many rights: freedom of expression, access to information, association with others, religious belief and practice, and assembly, for example. Surveillance can deepen the effects of discrimination, whether by discouraging the expression of one's sexual identity, or access to certain types of health information, or political association, or educational access. Unlike surveillance in the physical world, where resources for intensive data collection are limited (imagine tailing a suspect's

44 *Segerstedt-Wiberg and Others v. Sweden* [2006] ECtHR, App No 62332/00, [2006].

45 See European Parliament News: Q&A on EU Data Protection Reform (22 October 2013), available at http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform.

movements for a week) and collation of many different types of data is laborious, surveillance of digital information can be easy and collation of information cheap. Concerns that untrammelled surveillance can facilitate a 'police State' have been borne out historically, making lawful controls on State information gathering, if anything, more important to any democratic society in the digital age.

The human rights concerns with such programmes were featured in the April 2013 report of Special Rapporteur La Rue, just weeks before Edward Snowden's leaks were published. Noting that the digital revolution had both generated vastly more information about individuals, and made the means of surveillance vastly more cost-effective and unlimited by scale or duration, the Special Rapporteur raised the alarm that national legal standards needed to protect human rights were not keeping pace with technological developments. Of particular concern were national legal standards that impose little or no judicial oversight, or allow warrantless surveillance powers in the name of 'national security' without any particular demonstration of a genuine need or threat.[46]

Human rights concerns about excessive, secretive and inadequately supervised government collection, retention and surveillance of online information long predate the Snowden revelations,[47] but these have pushed the issue to the forefront once again. In addition to serious diplomatic concerns expressed to the US by many other governments, there is an outpouring of domestic administrative review and legislative proposals to place the US National Security Agency (NSA) surveillance under tighter controls. It is of concern in terms of the threat to human rights that many other governments have fewer controls on domestic State surveillance than the US, or require data retention by intermediaries for substantial periods of time, coupled with the ability of law enforcement agencies to access the retained data without judicial oversight.

Surveillance or monitoring of communications by the authorities or agents of another State is typically espionage. While espionage is usually a criminal offence in municipal law, there is generally a legal disconnect regarding peacetime espionage in international law, making an international rule of prohibition or permission difficult to articulate. Universally condemned and often punished, spying is also universally practiced against friend and foe alike. However, in terms of IHRL, to the extent that foreign surveillance is an unlawful or arbitrary intrusion on privacy and an inhibition on the freedom of expression and information, the State's responsibility to ensure rights to those within

46 Report of the Special Rapporteur 2013 (n 10) paragraphs 50-60.

47 The 'Snowden revelations,' still ongoing at the time of this writing, primarily indicate the revelations (whether initially by Edward Snowden or by subsequent sources) of massive data collection programs of the US National Security Agency (NSA), including those authorised by Section 215 of the *Patriot Act* (enabling, e.g., collection of business records, including bulk records of cell phone metadata) and Section 702 of the *Foreign Intelligence Surveillance Amendments Act* (enabling, e.g., large-scale collection of content of telephone and email communications relating to targets of investigation), that operate without Constitutional restriction against persons outside the US and that in operation also invade the records of millions of persons within the US), and secondarily follow-on information about surveillance programs of other countries.

its territory and control is activated. It follows that a State may not evade its own responsibility to stay within the limits on surveillance required by IHRL by facilitating unlawful or arbitrary surveillance on the part of another State with a view towards benefiting from information gained through what amounts to unlawful searches and seizures.[48]

The absence of a comprehensive international framework to protect the right to privacy from State surveillance has led the former Special Rapporteur on human rights and counter-terrorism, Martin Scheinan, to propose that the UN Human Rights Council initiate some 'soft law' standards via a global declaration on data protection and data privacy.[49] The need for the UN Human Rights Committee to update its General Comment on the right to privacy has also been noted,[50] and a recent conference of global data protection and privacy commissioners called for an Additional Protocol to Article 17 of the ICCPR to promulgate 'globally applicable standards for data protection and the protection of privacy.'[51] In this regard, two sets of principles recently issued by civil society expert groups may provide a basis for increasing consensus around standards. One is the Global Principles on National Security and the Right to Information ('The Tshwane Principles'),[52] endorsed by the Parliamentary Assembly of the Council of Europe,[53] which centre on transparency, respect for rights, and democratic accountability as a foundation of government information-gathering activities. The other is the International Principles on the Application of Human Rights to Communications Surveillance, which largely collect and restate general principles related to the right to privacy, transparency, and regulation of surveillance in international law.[54]

The introduction of a U.N. General Assembly resolution on the right to privacy in the digital age by Germany and Brazil may presage a gradual shift in the law, supporting a growing recognition that indiscriminate mass surveillance outside the territory of a State may constitute a violation of human rights. The resolution, which noted with deep concern the 'negative impact' of such practices on human rights, called for the issue to

48 Cf. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001), Articles 16 and 17, available at http://www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf.

49 Martin Scheinin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin* (UN GA Doc. A/HRC/13/37, December 2009), para 73.

50 Report of the Special Rapporteur 2013 (n 10) para 98; many human rights non-governmental organisations have also called for an update as well.

51 35th International Conference of Data Protection and Privacy Commissioners, *Resolution on anchoring data protection and the protection of privacy in international law* (Warsaw, September 2013), available at https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf.

52 Global Principles on National Security and the Right to Information (12 June 2013), available at http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

53 PACE Recommendation 2024 (2013), National security and access to information (2 October 2013).

54 Final version of 10 July 2013, available at https://en.necessaryandproportionate.org/text (the author's organisation has endorsed these, along with nearly 300 others).

be subject to forthcoming reports before the UN Human Rights Council and the General Assembly.[55]

7. Anonymity

The ability to communicate and associate with others without identifying oneself has been recognised in many contexts as essential to the exercise of free speech and association as well as to privacy. Anonymity is increasingly valuable to netizens, given the enormous amount of personal information that can be located and aggregated online, not to mention the vulnerability of gatekeeping hosts to official demands for disclosure. Anonymous speech is essential to dissidents with reason to fear persecution, but also to any resident of a democracy who wishes to participate in debate without having the discussion tied to other sensitive aspects of his or her identity, such as professional role, family, or religious affiliation. As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression wrote in April 2013:

> [R]estrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas. They can also result in individuals' de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities. Furthermore, restrictions on anonymity allow for the collection and compilation of large amounts of data by the private sector, placing a significant burden and responsibility on corporate actors to protect the privacy and security of such data.[56]

South Korea's experience in this regard is instructive. Following a series of well-publicised cyber-harassment incidents, South Korea legislated that all websites with more than 100,000 visitors a day must require users to create accounts using their national identification (ID) number. This in turn led to a small epidemic of prosecutions of people on 'false information' charges, leading Google to disable uploading comments onto Korean YouTube. The policy provoked further embarrassment when it became known in mid-July 2011 that some 35 million ID numbers (representing almost half the population) had been stolen from a major web portal company through an attack emanating from China.[57] Eventually the Constitutional Court struck down the real name policy in the *Act on Promotion of Information and Communications Network Utilization and Information Protection* on constitutional grounds of freedom of speech and the right to control personal information.[58]

---

55 UN General Assembly, Third Committee, Draft Resolution 'The right to privacy in the digital age', UN Doc. A/C.3/68/L.45/Rev.1 (20 November 2013) available at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.

56 Report of the Special Rapporteur 2013 (n 10) para 49.

57 Korea Herald, '35m Cyworld, Nate users' information hacked' (28 July 2011), available at http://www.koreaherald.com/view.php?ud=20110728000881.

58 Oiwan Lam, 'South Korea: Internet 'Real Name' Violates the Constitution,' Global Voices (28 August 2012), available at http://advocacy.globalvoicesonline.org/2012/08/28/south-korea-internet-real-name-law-violates-

It is important to recognise that the right to anonymity is far from absolute; indeed, there are often good reasons to require disclosure of identity, such as the investigation of crime and protection of public safety. Anonymous or pseudonymous communication has come under criticism as encouraging irresponsible speech that may have negative consequences for individual reputation and safety. Supporting real name use is entirely permissible, as a corporate, professional, State or best practice recommendation. At the same time, blanket requirements of real name registration, much like law enforcement efforts to collect identification without reasonable suspicion and a judicial warrant, do not meet the requirement that restrictions to rights be both necessary and proportionate in a democratic society.

8. Pressuring Intermediaries: Internet Service and Content Provider Liability

A distinctive feature of web 2.0 platforms is interactivity; the internet has facilitated an entirely new form of publishing, where readers may speak to each other in close to real time and, in turn, publish their material to a global audience without the mediation of a business that curates content. This has transformed the web into a genuine marketplace of ideas, enabling a vastly richer array of commentary and knowledge dissemination and association than ever before (not to mention enlivening the pastimes of teenagers and cat lovers, and facilitating brainstorming amongst those inclined to terrorism).

The regulation of cyberspace in many democratic countries already makes certain accommodations to this unique and valuable feature of online communication. In consideration of both the massive and rapid nature of data flows, the role of ISPs, web-hosts, and others who carry the flow is protected from the sort of immediate liability to which newspaper editors or broadcasters are subject. The importance of insulating carriers of third party content can hardly be overemphasised from a free expression perspective. Commercial intermediaries are the gatekeepers to cyberspace for most netizens, and their policies are sensitive to potential liability and shaped by national law. A duty to pre-screen for potentially illegal content throttles the internet as a medium for creative and controversial ideas, and reduces its value as a fairly instantaneous global means of communication and networking. Notice and take-down remedies will generally provide the 'safe harbour' for intermediaries, but can be defeated by narrow interpretation, as demonstrated by the conviction of Google executives in Italy on privacy intrusion, even when the offending video was removed within two hours of receipt of a police complaint, albeit two months after posting.[59] From the point of view of the originator of suspect content, the fact that companies can block content on

the-constitution/.

59 Rachel Donadio, 'Larger Threat is Seen in Google Case' *New York Times* (24 February 2010), available at http://www.nytimes.com/2010/02/25/technology/companies/25google.html?_r=2&pagewanted=all.

mere allegation of its unlawfulness is problematic. While newspapers will often fight and win against court injunctions, the major online intermediaries will usually take down content to minimise liability without even a court order, leaving the legal cost and trouble of litigating to their customers.

In this respect, the recent decision of the European Court of Human Rights in the *Delfi* case is particularly troubling.[60] Delfi, a news portal, hosted vulgar and threatening comments from readers, under a notice and take-down procedure. The Court found the company was liable for damages for defamatory comments, in light of a host of particular circumstances. These included that the company had taken no measures to enable the target of the defamation to identify the authors and pursue them; the fact the comments were in response to an article the company published, a context where it was alleged the company had moderated comments in the past; and the very modest damages assessed by the Estonian court. Despite this host of mitigating circumstances, the decision does not seem to give sufficient weight to both the need to allow anonymous online comment, the company's efforts in removing offensive material once on notice, and the likelihood that similar companies are likely to censor content much more vigorously following this judgment.

The role of internet companies in facilitating the bulk data collection and surveillance activities of the US government, and possibly other governments, is not well understood, in great part because such arrangements have been conditioned to secrecy about their existence. While some internet companies have voluntarily endorsed standards on transparency, issued transparency reports when possible, and even attempted to challenge government gag orders, the extent to which they are able to reveal or challenge government orders that they disclose customer information is opaque. The experience of Lavabit, a secure email provider that counted among its customers Edward Snowden, is disturbing, in that the company's founder saw no way to avoid US government demands to enable surveillance of all its customers other than by closing down the business entirely.[61]

9. Self-Help

Despite the growing body of both international cyber crime law and mutual legal assistance treaties to address criminal cyber actions, enforcement is often frustrated for many reasons, among them a lack of sophisticated technical ability in law enforcement, distrust of seeking help from government agencies (and giving them information about computer networks), the problems of addressing transnational crime, and lack of

60 See Case of *Delfi AS v. Estonia*, (Application no. 64569/09) 10 October 2013, available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{"itemid":["001-126635"]}.

61 Michael Phillips, 'Lavabit and the Right to Private E-Mail' *New Yorker* (11 October 2013), available at http://www.newyorker.com/online/blogs/elements/2013/10/lavabit-and-the-right-to-private-email.html.

political will. As malicious intrusions on networks increase, State failure to effectively deter or punish malicious cyber actions has led to calls for the legalisation of active self-defence measures on the part of private actors, or even the adoption of measures of retorsion or reprisal on the part of States.

From a human rights perspective, authorising cyber self-defence is problematic, in that it generally involves, at a minimum, an intrusion into the attacker's system and data, and often some harm, therefore inflicting a violation of rights in order to deter or punish a prior violation of rights. It is difficult enough for law enforcement to keep its responses to the minimum force necessary to stop a criminal suspect or act, and it is likely to be much harder for a wide range of non-State actors to exercise such discipline, not to mention foresight with respect to likely consequences. Matthew Waxman, writing about the complications of pursuing reprisal in the contest of armed conflict, raised many points with salience to human rights.[62] Attacks can be routed through intermediaries (for example, botnets), and attribution is often difficult or uncertain. Self-defence (a doctrine grounded in the reality of a physical fight where attribution is usually obvious) may not only inflict a parallel human rights violation but do so to the wrong person, a bystander or another crime victim. Lowering the bar on when an attack can legally justify active self-defence measures can simply encourage swifter resort to 'force' on all sides. Ultimately, the fascination with self-defence reflects a deep distrust in the State's ability and willingness to protect rights, and the lack of a strong international framework for rights protection. This is not a healthy situation, and argues for greater international commitment to protecting human rights and agreeing on universal standards to secure the integrity and privacy of online communications, networks and data. It also tends to lend strength to the idea that passive self-defence, that is, measures such as strong encryption to deter would-be attackers, is probably the better investment for supporting rule of law. To that end, governments would do well to shift focus from trying to ban or compromise privacy measures such as the free anonymisation software 'Tor' to using judicially supervised standards in law to compel decryption where that is both necessary and the least intrusive means of protecting public order or national security against the threats posed by specified targets.

10. Expanding Powers, Expanding Obligations

One of the key issues raised by the NSA surveillance practices, and the limp (and largely secret) oversight of the US Foreign Intelligence Surveillance Court, is the exclusion of foreigners living abroad from US constitutional protections against search and seizure. The disregard of the US for the privacy rights of millions beyond its borders has caused public uproar, particularly in allied countries, yet it is not clear that other governments

62 Matthew C. Waxman, Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions 89 INT'L L. STUD. 109 (2013), available at http://ssrn.com/abstract=2235838.

conceive of their human rights duties as global in reach when it comes to national security surveillance.

The issue can be approached as a matter of US intrusion on the sovereignty of other States, though it appears that in at least some cases the collection of data was done with the acquiescence and assistance of the foreign State, and in many cases the interception was done at a point where communications passed through US facilities or territory. There is also the difficulty that alternative approaches to justifiable and necessary surveillance or data acquisition (for example, by recourse to mutual law enforcement treaties or similar cooperation measures) would likely be unavailable with regard to less friendly countries.

A more straightforward approach might be to consider the nature of the activity under the lens of IHRL, and particularly the standards of the ICCPR, a treaty to which 167 States are party. Under Article 2(1) of the ICCPR, States are required to 'respect and to ensure to all individuals within its territory and subject to its jurisdiction' the rights of the Covenant, including privacy and freedom of expression. The Human Rights Committee for many years has been clear that it interprets this requirement as disjunctive benefitting persons that are either within a State's territory or within its jurisdiction, which it has interpreted in General Comment 34 as including 'anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.'[63]

The question then becomes one of interpreting 'effective control' or 'jurisdiction.' To the extent that one State conducts surveillance of another State's residents by means of facilities located on its own territory, this could be an instance where their communications and data fall within that State's jurisdiction. Another approach might be to posit that a State that regularly permits another State to exercise the authority of mass surveillance over its population has delegated effective control over that aspect of the population's rights. Where one State over time fails to fulfil its responsibility to ensure rights to privacy and free expression to its residents, such that another State may conduct mass surveillance with impunity, this could also be taken as evidence the other State is the one that exercises 'effective control' over at least this crucial aspect of individual personality and autonomy.[64]

63 HRC, General Comment No. 31 (n 13) para 10.

64 The European Court of Human Rights, in the *al-Skeini* case noted an exception to the usual principle of jurisdiction as territorial when a State's agents produce effects outside its own territory, as when with the acquiescence of the territorial State, another State's authorities exercise 'all or some the public powers normally to be exercised by that Government.' This might include carrying out 'executive or judicial functions on the territory of another State'. ECtHR Grand Chamber, *Case of al-Skeini and Others v. The United Kingdom*, (Application no. 55721/07) 7 July 2011, paras 134-135; see also De Schutter, Eide, Khalfan, Orellana, Salomon and Seiderman, 'Commentary to the Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights', Human Rights Quarterly 34 (2012) 1084, commentary to Principle 9 (with thanks to Ian Seiderman for these references).

This approach is not quite as novel as it seems in light of the increasing tendency to interpret custody of an individual as 'effective control' over that person for purposes of obligations under the ICCPR. While the physical aspects of any individual are located in a particular jurisdiction, our freedoms and identities increasingly reside where our data travels, and those governments that take custody of it for any purpose take custody of so many aspects of our personality as to have our thoughts, beliefs, livelihoods, histories, associations, movements and reputations within their effective control. Just as the internet has conferred enormous power to individuals over their lives, so too has it handed enormous power to States over individuals. With power comes responsibility, including the responsibility to protect human rights as an essential component of human security.

Ian Walden

International Telecommunications Law, the Internet and the Regulation of Cyberspace

Over the years there has been considerable debate, confusion and uncertainty about the most appropriate response to the question: who controls the internet? Partly this results from the scope of the term 'internet', which is widely used to encompass not only the 'network of networks' that comprises the transmission platform for communications, but also the content, applications and services that we access and use over that platform: the metaphorical terrain which is commonly referred to as 'cyberspace'. This chapter examines the role of international telecommunications law in the governance of the former, the 'network of networks', or more specifically internet communications, and its indirect role in the governance of the latter, cyberspace.

In terms of legal sources, telecommunications legal regimes exist at national, regional and international level. Where appropriate, reference will be made to issues that have arisen, and measures that have been taken, at a national and regional level that reflect or shape developments in international telecommunications law. However, the focus of this chapter is on the impact and influence of two key intergovernmental organisations, the International Telecommunication Union (ITU) and the World Trade Organization (WTO), and the various instruments of public international law for which they are responsible. Together, these legal instruments have helped to shape the telecommunications industry and markets around the world, within which the network of networks has arisen.

In the minds of some, the ITU is antithetical to the development of the internet because it is representative of the interests of the State and has a desire to centralise control, in contrast to the market-led and anarchic growth of the internet and cyberspace. The reality is inevitably more complex, with ITU activities making important contributions to the development of the internet in a number of areas, particularly in terms of standards-making. On the other hand, the WTO presides over a series of trade agreements, as well as an ongoing process of trade liberalisation, which is widely recognised as supporting the globalised telecommunications infrastructure that underpins the internet. However, as the attention of the trade community has shifted from infrastructure to more content-related service sectors, further progress has stalled, in part perhaps a reflection of the more complex nature of the policy concerns that arise in relation to the regulation of cyberspace.

1. Telecommunications Law

The first issue for consideration is to define what is meant by 'telecommunications law', distinguishing the field from the other areas of law examined in this book. Telecommunications law and regulation are concerned with the provision of telecommunication networks, services and equipment. Telecommunication networks, whether comprised of wireline or wireless components, fixed or mobile, constitute the infrastructure that enables the transmission of signals, data and content. Telecommunication services are the form in which we obtain access to the networks and permit us to send and receive communications. Telecommunications equipment encompasses any device, from computer to mobile phone, which enables us to communicate over the networks, through the provision of services.

Telecommunications equipment also includes the hardware and software that comprise a network, but this is generally regulated under network rules. The devices that connect to networks, at the edge, from web servers to handsets and operated by public, commercial or individual end-users are variously referred to as 'telecommunications terminal equipment' and 'customer premises equipment'.[1] The rules governing the manufacture, marketing and connection of such equipment, whilst one strand of telecommunications law, are relatively stable, straightforward and do not impinge substantially on the cyberspace environment, and are therefore beyond the scope of this chapter.

The laws and regulations that govern the provision of telecommunication networks and services are a relatively recent phenomenon in terms of the scope and range in which we currently experience them. Laws governing our means of communications, such as postal services, obviously have a long history, but it was the liberalisation of national telecommunications markets in the 1980s that resulted in the burgeoning array of laws and regulations that comprise modern telecommunications law. Prior to liberalisation, the monopolist provider of telecommunication networks, services and equipment was a branch of the executive of the State in all countries except the United States (US), and therefore the need for rules was limited. Liberalisation has brought forth a complex body of telecommunications law designed to address either economic, social or public interest policy objectives.

Laws are required to regulate the telecommunications market: firstly to address the legacy of the State-owned monopolies, whether subsequently privatised or continuing to operate under public ownership. Secondly, unique features of the market mean that approximating a fully competitive marketplace may always require State intervention, not least because in such networked industries competitors are also customers. In terms of social policy, access to telecommunications is recognised as being of fundamental importance to a nation's citizens, similar to other utilities,

1 EU Directive 99/5/EC (OJ L91/10, 7.4.1999), Article 2(b) and 47 USC § 153(16) respectively.

which can require intervention to ensure the availability and provision of a certain minimum level of services at an affordable price, the so-called universal service policy. Sectoral consumer protection and data protection measures are likewise often viewed as necessary in the telecommunications sector due its unique characteristics. A final driver for telecommunications law is its role as a facilitator of communications, which inevitably makes it of interest to governments, law enforcement agencies and others who may want to control such communications, for good or ill, including for identifying those engaged in unlawful activities. This area is becoming of increasing relevance both to the telecommunications sector, to internet providers and to those operating in cyberspace.

A critically important feature of telecommunications law is the near universal establishment of a regulatory authority to carry out oversight and intervention of the telecommunications sector. Such regulation may be carried out by the executive, through a departmental ministry, but more often the function will reside with an independent authority, independent not only of market participants, but also of government, to the extent that they continue to own the incumbent operator, in whole or part. Telecommunication regulators may have law-making powers, exercise judicial functions or simply encourage best practice. However, their on-going interactions with providers and interventions in the sector mean that fundamental to an understanding of telecommunications law is recognition of the role and conduct of regulators.

2. Cyberspace and the Regulated Sphere

Having defined the scope of telecommunications law, it is necessary to consider how such rules interact or impact on what is referred to in this chapter as 'cyberspace'. Cyberspace is often viewed as sitting on top of the telecommunications layer, although the reality is considerably more blurred. To connect to the internet, we require an underlying transmission service, which is governed by telecommunications law. The content we communicate and the services we consume generally fall outside the regulated sphere, although the dividing line between the two can be the subject of considerable debate in terms of legal characterisation.

Our earlier definition of telecommunications law is clearly not suitable as a statutory definition, as it is incapable of delineating between a regulated activity and that which falls outside the regulated sphere with sufficient clarity to meet the requirement of legal certainty in accordance with the Rule of Law. Legal definitions are found in international, regional and national instruments, of which the following is from European Union (EU) law:

> '[E]lectronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services

> and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.[2]

This concept adopts a technical approach, focusing on the conveyance of signals as the regulated conduct, rather than a subjective approach based on the imputed intention of a service provider or a consumer's perceptions. One boundary lies where a service consists 'mainly' of non-conveyance activities, although we are given no guidance as to whether to adopt a quantitative or qualitative approach. A second boundary is drawn where the service involves 'editorial control' over any content being conveyed. Both regulatory boundaries can generate uncertainties when applied in a cyberspace environment.

Two examples will serve to illustrate the potential complexities involved. First is 'WhatsApp', which describes itself as a 'cross-platform mobile messaging app which allows you to exchange messages.'[3] To use the application, a user needs a separate transmission service such as a public Wireless Fidelity (Wifi) connection or a mobile internet data service. While the latter is clearly a telecommunication service, how should the application itself be characterised? One approach would be to say that, since it resides on the user's device it is not a service *per se* and forms part of the terminal equipment, and thus falls outside the regulated sphere. Alternatively, however, the primary function of the application is the 'exchange of messages' by handling user content in a particular way to enable their efficient transmission over the underlying transmission service. A third approach is to consider user expectations; if users perceive 'WhatsApp' to be a communication service, it should be regulated as such.

Second, to protect their networks and services, as well as their customers, telecommunication providers deploy various software-based tools to detect and block the transmission of certain types of content, from unsolicited emails (so-called 'spam') to viruses and associated malware. Such tools form part of the overall service and may operate on the basis of monitoring the attributes of communications or by interrogating their content. Either way, the effective result of using these techniques is to control the content being transmitted over telecommunication networks and services, which could be viewed as the provider taking a certain responsibility in respect of the content transmitted over the service, akin to editorial control, and taking the conduct outside the scope of the regulated sphere.

These examples illustrate that while telecommunication law may be designed to distinguish the regulation of conveyance from the content being carried over such networks, the distinction will not be clear cut, which has obvious implications for the

---

2 Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (OJ L 108/33, 24.4.2002), at Article 2(c).

3 See http://www.whatsapp.com/.

regulation of cyberspace. Such blurring is most obvious in the current debates over net neutrality.

3. Net Neutrality

The net neutrality debate encompasses a wide range of issues and concerns. Some are specific to particular jurisdictions, while others are more universal. At its most basic, net neutrality concerns the treatment by the underlying networks that comprise the internet of the multitude of content, applications and services that are carried over those networks. Historically, the internet operated on a best efforts non-discriminatory basis, treating all packets equally. As the internet has become the dominant communications platform, issues have arisen concerning the extent to which networks can, and should, interfere with the flow of packets transmitted across them, whether prioritising, degrading or blocking content, applications or services, rather than on an open non-discriminatory basis. To the extent that any discrimination results from traffic management techniques designed to improve overall network performance and quality of service, it is broadly accepted as a necessary technical feature. However, where controls are exercised for commercial reasons, such as degrading traffic throughout from competitive services, or for policy reasons, such as inhibiting the use of peer-to-peer applications (e.g. BitTorrent) that are seen as tools for widespread copyright infringement, there are concerns about social access and utility, transparency, anti-competitive behaviours and infringements of individual and consumer rights.[4]

Regulatory responses to net neutrality concerns have varied greatly between jurisdictions. In the US, the Federal Communications Commission (FCC) has acted on specific discrimination complaints from market participants,[5] while attempting to lay down general regulatory principles, although it has faced on-going challenges to its lawful authority to impose such rules.[6] The FCC's Open Internet Order[7] is based on three key rules: transparency, no blocking and no unreasonable discrimination. With respect to the blocking rule, greater flexibility is given to mobile broadband providers on the grounds that they are subject to greater technical constraints due to their use of the electromagnetic spectrum. For fixed-line providers, the obligation is 'not to block lawful content, applications, services, or non-harmful devices, subject to reasonable network management'.[8]

4 See generally Marsden, C., 'ISPs: Content Liability, Control and Neutrality', Chapter 15, in *Telecommunications Law and Regulation* (Ed. Walden), OUP 2012.

5 E.g. FCC investigation of Madison River Communications (2005).

6 See *Comcast v* FCC, 600 F.3d 642 (2010).

7 December 2010.

8 *Ibid.*, at § 8.5.

In Europe, the response to date has been somewhat more muted, with initial rule-making focusing on the consumer protection aspects of the debate, requiring transparency for end-users and enabling the imposition of minimum quality of service standards.[9] Discriminatory issues between operators have been left to sectoral regulators to address through either *ex ante* or *ex post* competition powers. In September 2013, new proposals were published by the European Commission that would allow the provision of tiered access to the internet with respect to specialised services,[10] which has generated controversy among certain sectors of internet users for conceding the net neutrality principle.

In the author's opinion, net neutrality is likely to dissolve over the coming decade into a component of universal service policy rather than remain an objective in its own right. Universal service is the desire of governments to ensure that all get access to communication networks and the services made available over them, regardless of socio-economic status or geography. A minimum quality of service made available to all at an affordable cost, facilitated thorough regulatory intervention, such as setting standards, and the financial support of governments through subsidies. However the net neutrality debate develops in the future, what is clear is that the operation of cyberspace as we know it is dependent on the underlying networks, which are subject to regulation under telecommunications law regimes.

4. International Telecommunications Law

In the early days of cyberspace, it was suggested by some that cyberspace transcended national territories and therefore sovereignty and traditional laws were no longer applicable.[11] The fundamental mistake of such assertions was in seeking to divorce the virtual space in which people operated in cyberspace from the physical resources, computers and networks over which cyberspace operated. That control could be, and was, exercised over these physical resources and the persons that owned and operated them, meant the inevitable demise of such cyberlibertarian ideals. However, a second level of misunderstanding represented by such sentiments was the implication that national laws were all from which cyberspace need to be liberated. As this book illustrates, there is plenty of international law that is applicable to cyberspace, irrelevant of whether any particular State's law are applicable. This is particularly true in the area of telecommunications law. As an inherently trans-national technology, international agreements enabling the building and operation of international networks date back

9 Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (OJ L 337/11, 18.12.2009).

10 Proposal for a Regulation 'laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent' (COM(2013) 627 final, 11.9.2013), at Article 23(2).

11 John Perry Barlow, A Declaration of Independence for Cyberspace (1996), http://w2.eff.org/Misc/Publications/John_Perry_Barlow/barlow_0296.declaration.txt.

some 150 years to when 20 European States signed the International Telegraph Convention in 1865, which ushered in the 'Victorian Internet'[12] and eventually evolved into the inter-governmental organisation, the ITU.

International telecommunications law can be divided into different sources of rules. First, there are laws governing the building of international networks. International networks primarily comprise satellite systems and submarine cables, both covered elsewhere in this book and subject to distinct international rules, specifically space law and the law of the sea.[13] Second, through instruments of public international law, national government commit and submit themselves to an international legal order, accepting obligations to conduct themselves in certain ways, especially with respect to the treatment of other nations. Whether such laws can be enforced against non-compliant States will vary by regime as well as being subject to realpolitik, but nonetheless they represent a form of law. Third, in order for national networks to interconnect and transmit information, they need to communicate in accordance with agreed standards operating at numerous technical levels, which can be viewed as a common language. While international standards are not in themselves law, rules exist at a national, regional and international level that imposes obligations on providers to implement or comply with such standards. A fourth source of international telecommunications law is from development organisations, such as the World Bank and the European Bank for Reconstruction and Development, which promulgate and impose international telecommunications norms and best practices upon developing countries in receipt of aid and investment under loan and related financial agreements.

The following sections examine the second of these areas of law and the international agreements and inter-governmental institutions established under them, specifically the ITU and the WTO.

4.1 International Telecommunication Union

The ITU was founded in 1932, through the merger of the International Telegraph Union and the International Radiotelegraph Union, although its origins date back to the establishment of the International Telegraph Union in 1865.[14] As such, the ITU is one of the oldest intergovernmental organisations, which illustrates the inherently international nature of the telecommunications industry, both in terms of the scope of services being demanded and the nature of the physical resources involved, specifically

12 Standage, T., *The Victorian Internet*, Phoenix, 1998.

13 See further Martha Mejía-Kaiser, 'Space Law and Unauthorised Cyber Activities' and Wolff Heintschel von Heinegg, 'Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law', both in this volume.

14 For a detailed history of the ITU, see Lyall F., and P.B.Larsen, *Space Law: A Treatise*, Ashgate, 2009: pp. 200-206.

the radio spectrum. It became a specialised agency of the United Nations in 1947.[15] Based in Geneva, the ITU exists to further the development of telegraph, telephone, and radio services, to promote international cooperation for the use of telecommunications and the development of technical facilities, and to allocate radio frequencies. The basic principles for the conduct of international telecommunication services, the basis for membership of the ITU and its organisation and permanent organs, are contained in the *Convention* and *Constitution of the International Telecommunication Union*.[16]

The Constitution contains the fundamental principles of the ITU, while the Convention details the operational procedures, which may be subject to periodic review. The work of the Union is sub-divided into three sectors:

- Radiocommunication Sector (ITU-R);
- Telecommunication Standardization Sector (ITU-T); and
- Telecommunication Development Sector (ITU-D).[17]

The work of each sector is carried out by a series of organisational entities: world and regional conferences, boards, assemblies, and numerous study groups examining particular topics.

The ITU has two categories of membership:

- Member States, i.e. national governments, of which there are currently 193, although governments may designate national regulatory authorities as their representative;[18] and
- Sector Members, representing all the various categories of players within the telecommunications industry, including regional and international organisations, such as the Internet Society and the Groupe Speciale Mobile (GSM) Association. In total, these entities number over 700.[19]

Sector Members have been involved in the work of the ITU since the Rome Telegraph Conference in 1871, with the sponsorship of a Member State (Convention, Article 19(1)(a), (b)). In 1998, the Convention was amended to enable Sector Members to apply directly to join the ITU; although the applicant's Member State must approve such a procedure.[20] However, despite being eligible for membership since 1871, it was not until the Plenipotentiary in 1994 that Sector Members were able to formally participate in

15 *International Convention on Telecommunications*, Atlantic City, 2 October 1947; 1950 UK Treaty Series No 76, Cm 8124.

16 See the *Constitution* and *Convention of the International Telecommunication Union*, Geneva, 22 December 1992. The following text is based on the Constitution and Convention as of 1 January 2012.

17 Constitution, Article 7.

18 E.g. Ofcom in the case of the UK.

19 See http://www.itu.int/en/membership/Pages/sector-members.aspx.

20 Convention, Article 19(4*bis*)-(4*quater*).

the decision-making processes of the ITU; and only in 1998 that Sector Members were recognised as having formal rights of participation under the Constitution.[21]

Under the Convention, the ITU Secretariat has obligations to 'encourage the enhanced participation' of Sector members (Article 19), while a Sector Member may also be authorised to act on behalf of a Member State (Convention, Article 19(9)), which may be the case where an operator continues to be part of the Government, often under a specific ministry, or has been conferred with certain special or exclusive rights within the jurisdiction. Sector Members participate in those sectors of the ITU for which they apply, e.g. ITU-R, so participation in one sector does not confer authorisation to participate in another.

Despite the enhanced status of the Sector Members, the fundamental legal instruments of the ITU, the Constitution, Convention, and *Administrative Regulations*, continue to be under the exclusive jurisdiction of the Member States.

An industry player may also be invited by a Sector of the ITU to participate as an Associate within a study group (Convention, Article 19(12)), with more limited rights of participation, although with an obligation to help defray the costs of the group in which they participate (Convention, Article 33(5)(4*bis*)). This category of participant was established within the ITU system in 1988, as a means of enabling participation by small entities in the work of the ITU.

With the liberalisation of the telecommunications industry and the proliferation of commercial operators, tension has grown within the ITU over the position of industry members within the ITU structure. On one hand, governments are wary of relinquishing their historic rights to control the organisation; on the other, they recognise industry's legitimate interests in the work of the Union, as well as wanting industry to contribute any ever greater proportion of the costs associated with its operations and activities.[22] The issue of industry involvement dominated the 1998 Plenipotentiary Conference in Minneapolis, where a single category of industry membership was finally recognised: '*Sector Member:* An entity or organization authorized in accordance with Article 19 of the Convention to participate in the activities of a Sector' (Constitution, Annex).

In terms of financing the work of the ITU, the Constitution was amended to place Sector Members' contributions on an equal footing to those of Member States (Article 28). In addition, new Advisory Groups were established for each Sector with a broad remit to review the 'priorities, programmes, operations, financial matters and strategies' of the various bodies within each Sector.[23] These new bodies increase the influence of Sector Members within the ITU as Member States and industry participate on an equal footing.

21 *Ibid*., Article 3(3).

22 See Resolution 110 (Marrakesh, 2002): 'Review of the contribution of Sector Members towards defraying the expenses of the International Telecommunication Union'.

23 Convention, Article 11A, 14A, 17A.

As part of a broad review of the ITU's role and strategy for the future, an ITU Reform Advisory Panel was established at the end of the last decade, comprising both governmental and private sector members.[24] It made the following recommendation in 2000 with respect to the balance of influence between Member States and Sector Members within the ITU: 'The decision-making functions of the ITU should reflect the modern, competitive telecommunications environment in which the private sector plays the lead role while the regulatory agencies act as an arbitrator for the wider public interest.'[25]

Whilst such sentiment was welcomed by the telecommunications industry, the degree to which Member States continue to intervene in the sector in the public interest may give cause for concern. Currently, there are no institutional procedures to enable Sector Members to appeal against a decision made by Member States or arbitrate in a dispute with a Member State.

Constitution and Convention

As an international treaty, the Constitution and Convention of the ITU are legal instruments to which Member States are bound in respect of all telecommunications activities that 'engage in international services or which are capable of causing harmful interference to radio services of other countries'.[26] Whilst primarily detailing the rules governing the establishment and operation of the ITU, the Constitution also embodies certain fundamental legal principles governing international telecommunications in Chapter VI, which are potentially applicable to aspects of cyberspace.

The Constitution defines telecommunications as '[a]ny transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.'[27] Under the Constitution, Members give recognition to 'the right of the public to correspond by means of the international service', including a requirement that 'the services, the charges and the safeguards shall be the same for all users in each category of correspondence without priority or preference';[28] wording which would not be out of place in current debates on net neutrality.[29] Member States also have an obligation for 'ensuring the secrecy of international correspondence', although subject to a broad right of States 'to communicate such correspondence to the competent authorities in order to ensure the application of their national laws'.[30] Such an interception right has obvious echoes with

24 For a full list of Members, see http://www.itu.int/newsroom/reform/rapmembers.html.

25 ITU Reform Advisory Panel (RAP), Observations and Recommendations for Reform, 10 March 2000.

26 Constitution, Article 6(1).

27 *Ibid*., Annex at 1012.

28 *Ibid*., Article 33.

29 See section 3 above. See also Marsden, C., *Net Neutrality: Towards a Co-regulatory Solution*, Bloomsbury, 2010.

30 *Ibid*., Article 37.

the recent disclosures about the activities of US and United Kingdom (UK) intelligence agencies under the XKeyscore and Tempora internet surveillance programs.[31]

The majority of the principles, however, represent reservations that Members have the right to exercise over communications, especially concerning the right to 'stop' or 'cut off' transmissions 'which may appear dangerous to the security of the State or contrary to its laws, to public order or decency'.[32] This would clearly permit a State to block internet communications, as well as to monitor and filter traffic. Interestingly, where a transmission is stopped, notification should be given to the 'office of origin', potentially either the sender or the sender's service provider, except where it involves a matter of national security. Such transparency should facilitate accountability, although clearly not complied with by national operations such as the so-called Great Firewall of China. Finally, Member States are protected from any liability arising from the use of international telecommunication services,[33] which either reflects or is the source of the historic concept of common carrier protection from liability. At the end of the last century, this concept fed into the debates about the liability of internet service providers (ISPs), which resulted in the widespread adoption of statutory safe harbours from liability for certain forms of ISP conduct, such as 'mere conduit'.[34]

There are three unique features of the ITU Constitution and Convention that differ from traditional instruments of public international law. First, the private sector has a specified role in decision-making activities of the ITU, as noted above. Secondly, to ensure legal certainty, *Administrative Regulations* have a fixed date for implementation and have immediate provisional application unless the revision is formally refused by a Member State (Constitution, Article 54, 3*penter*). In addition, a Member State is deemed to have consented to be bound by the revision to the *Administrative Regulations*, after a period of three years, if it fails to notify the Secretary-General otherwise (Constitution, Article 54, 5*bis*). Thirdly, any reservations by a Member State have to be raised prior to the signing of the final acts of a plenipotentiary, since subsequent reservations are not possible. These provisions are designed to ensure legal certainty, which impacts directly on technical implementation issues.

Complementing the Constitution and Convention are *Administrative Regulations*, sub-divided into the *International Telecommunications Regulations* and the *Radio Regulations*. The *Administrative Regulations* comprise the general principles to be observed in the provision of international telecommunication services and networks, and the assignment and use of frequencies and orbital slots. Such Regulations 'shall

31 See http://articles.software.informer.com/prism-tempora-xkeyscore-what-is-it.html.

32 Constitution, Article 34.

33 *Ibid*., Article 36.

34 See, for example, Directive 00/31/EC on electronic commerce (OJ L178/1, 17.7.2000), Article 12 and 47 U.S.C. § 230(c)(1): 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'.

be binding on all Member States'.[35] At the time of accession to the Constitution and Convention, a Member State may make reservations in respect of any of the existing *Administrative Regulations* (Article 54(2)). Any subsequent partial or complete revision of the *Administrative Regulations* requires a Member State to indicate its consent to be bound, by depositing an instrument of ratification, acceptance or approval or by notifying the Secretary-General (Article 54(3)*bis*); although a Member State will be provisionally bound from the entry into force of the revision, if the Member State has signed the revision (Article 54(3)*penter*).

Under the Constitution, Member States are also required to:

> take the necessary steps to impose the observance of the provisions of this Constitution, the Convention and the Administrative Regulations upon operating agencies authorized by them to establish and operate telecommunications and which engage in international services or which operate stations capable of causing harmful interference to the radio services of other countries. (Article 6(2))

However, this blanket provision is qualified by the concept of a Recognized Operating Agency (ROA):

> Any operating agency [...] which operates a public correspondence or broadcasting service and upon which the obligations provided for in Article 6 of this Constitution are imposed by the Member State in whose territory the head office of the agency is situated, or by the Member State which has authorized this operating agency to establish and operate a telecommunication service on its territory. (Constitution, Annex)

Historically, ROAs were generally the State-owned incumbent operator but in a liberalised market, which is the position on the majority of member countries, the categories of ROAs can extend to any provider of international services, including internet service providers.

International Telecommunications Regulations

The current applicable *International Telecommunication Regulations* (ITRs) are those adopted at Melbourne in 1988; comprising some 10 substantive articles and a series of appendices.[36] Reiterating the Constitution, the ITRs are only binding on administrations, i.e. Member States and recognised operating agencies. Two provisions have been of particular importance over the subsequent years: Articles 6 and 9. Article 6, together with Appendix 1, outlines an international accounting regime for the carriage of international traffic. Since 1988, the application, validity and therefore

35 *Ibid*., Articles 4(3), 54.

36 Available at http://www.itu.int/ITU-T/itr/files/ITR-e.doc. They entered into force on 1 July 1990.

relevance of the regime has been substantially undermined by liberalisation of the global telecommunications market and the emergence of alternative calling procedures that by-pass such arrangements, such as internet telephony services like Skype. Conversely, Article 9 grants administrations the flexibility to enter into 'special arrangements' for the provision of international telecommunications networks and services. This provision has enabled Member States to tailor national and regional laws to reflect the evolving policy of a liberalised market, such as the application of interconnection regulations to intra-EU traffic, while ROAs have had the freedom to enter into private agreements that have effectively established an alternative regulatory environment which has been particularly relevant to the explosive growth of the internet.

Over the years there have been inevitable calls for the ITRs to be revised, reinterpreted or abrogated, with, in the latter case, the provisions of continuing relevance being transferred into other ITU instruments, such as the Constitution. These calls for reform have been driven, in part, by the considerable changes that have occurred in the market since 1988, but also by developing national concerns that the ITRs are too favourable towards richer nations and the dominant global players they represent. At the 1998 ITU Plenipotentiary, a resolution was adopted instructing the Secretary-General to establish an Expert Group to advise on the future of the ITRs.[37] No consensus on the way forward was reached by the following Plenipotentiary in 2002, or by the 2006 Plenipotentiary.[38] However, the 2006 Resolution provided an end date on the negotiations, by resolving that the ITU was to convene a conference in 2012 to decide on recommendations to amend the ITRs. The World Conference on International Telecommunications (WCIT) was duly held in Dubai, United Arab Emirates, in December 2012.

In the lead up to the WCIT, Member States submitted their proposals for reform of the ITRs, representing a broad spectrum of opinion from no change to radical expansion.[39] One proposal for reform, representing the perspective of certain developing countries, was to give greater granularity to the ITRs by incorporating references to various ITU recommendations in the ITRs, which would then become *de facto* mandatory for Member States. Such an approach was strongly resisted by countries such as the US who believe that such intervention in a liberalised market would be inappropriate. Other reform proposals focused on cyber security issues, expanding on existing harm-based obligations,[40] which raised concerns about the desire of some governments to exercise greater control over the internet.[41] Industry, both market participants and their customers, were particularly concerned that any substantial reform of the ITRs could

37 Resolution 79 (Minneapolis, 1998): 'International Telecommunication Regulations'.

38 See Resolution 121 (Marrakesh, 2002) and Resolution 146 (Antalya, 2006).

39 See ITU CWG-WCIT12/TD-43, 'Draft compilation of options', 24 November 2011.

40 ITRs at Article 4.3(a) and 9.1(b).

41 See, for example, McDowell, R., 'The U.N. threat to Internet freedom', *The Wall Street Journal*, 21 February, 2012.

undermine the growth and innovation that the sector has experienced over the last quarter of a century.

The outcome of the WCIT was a revision of the ITRs,[42] which will come into force on 1 January 2015 (Article 14.1). However, the final agreement did not command consensus amongst the voting States, with only 89 of the 144 Member States willing to sign the revised text; the non-signatories included most developed nations, including the US and the EU Member States. As such, the ITRs (2012) will only achieve partial adoption, unless subsequent discussions are able to bridge the gap between the parties.

Of the numerous proposals for reform, the final text includes relatively few distinctly new provisions, compared to amendments made to the existing text. Inserted into the Preamble of the ITRs is a commitment by Member States to respect their human rights obligations. The applicability of the ITRs was also extended to all 'authorized operating agencies' in a Member State.[43] Article 1 expressly limits the purpose and scope of the Regulations, stating that they 'do not address the content-related aspects of telecommunications.' However, a new provision is inserted calling upon Member States to take 'necessary measures to prevent the propagation of unsolicited bulk electronic communications'.[44] On the face of it, reconciling these latter provisions can appear problematic, since determinations about whether a communication is unsolicited or not would seem to require either some knowledge of the content of the communication or of the mind of the sender and receiver of the communication; both of which would seem beyond the appropriate remit of the Member States to interfere in. Conversely, the ITU has already adopted various technical recommendations on countering spam,[45] which reflects an acceptance that network-level measures can be an important component in tackling spam.

The 2012 revision of the ITRs has generated massive interest and controversy, much of it concerning the prospect of greater regulation over cyberspace activities, rather than the internet as a network of networks. Inevitably, much of the noise reflected broader political and economic interests that did not meet the reality of the wording being negotiated and adopted in the ITRs; however, the long term implications of the revision are yet to emerge.[46]

---

42 Final Acts of the World Conference on International Telecommunications (Dubai, 2012), available at http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.

43 *Ibid*., Article 1.1 b).

44 *Ibid*., Article 7.

45 See, for example, X.1241 (04/2008), 'Technical framework for countering email spam', available at http://www.itu.int/rec/T-REC-X.1241-200804-I.

46 See Hill, R., 'WCIT: failure or success, impasse or way forward', pp. 313-328, *International Journal of Law and Information Technology*, vol. 21, no. 3, 2013.

Radio Regulations

The Radiocommunications Sector of the ITU exercises a regulatory function in respect of the use of two scarce international resources, radio-frequency spectrum and orbital slots, both of which require management in order to maximise their use, as well as to prevent interference between services and space objects.[47] The primary legal instrument is the *Radio Regulations* (RRs), with the current version being adopted in 2008.[48] The RRs are contained in four volumes comprising some 59 articles, 25 appendices, and various resolutions and recommendations.

The RRs distinguish between three distinct acts in relation to frequency: allocation, allotment, and assignment (RRs, Article 1, 1.16–1.18). Allocation consists of an entry in the Table of Frequency Allocations for use in respect of one or more terrestrial or space radiocommunication services. Such services may be categorised as primary or secondary services, on a regional or global basis, with the latter being required to comply with the interference rules laid down for the former, although being unable to claim protection from interference from the former. Allotment indicates the use of a designated frequency by administrations for a service in certain countries or geographical areas and under specified conditions. The assignment of frequencies is carried out by Member States, under their sovereign authority, through an authorisation or licensing procedure. When granting an assignment, Member States are free to derogate from the ITU allocation, but only to the extent that it does not cause harmful interference to others operating in accordance with the RRs (Article 4.4).

The procedures under the RRs are designed 'to eliminate harmful interference [...] and to improve use made of the radio-frequency spectrum'.[49] The overriding objective of the ITU regulatory regime is the efficient use of the spectrum, while ensuring that public safety and emergency communication services, the only other policy concerns directly addressed in the *Radio Regulations*, are not adversely affected. The ITU regime is not, therefore, a comprehensive governing framework for the provision of radiocommunication services, since national and regional policies and laws on radiocommunications will generally encompass a much broader remit of issues, including environmental concerns.

---

47 Constitution, Article 1(2)(a), (b); Chapter II (Articles 12–16) and Convention, Section 5 (Articles 7–12). The ITU's procedures cover both geostationary and non-geostationary satellite systems.

48 The WRC-12 was held in Geneva, 23 January-17 February 2012, at which further revisions to the RRs were agreed.

49 Harmful interference is defined as '[i]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations.' Constitution, para 1003. See also the *Radio Regulations*, at Article 1(1.169). 'Harmful interference' is distinguished from 'permissible interference' (i.e. interference which falls within certain parameters) and 'accepted interference' (i.e. interference greater than certain parameters, but accepted by two or more administrations).

The ITU is also the forum for Member States to debate the allocation or reallocation of newly or prospectively available spectrum. In November 2007, for example, at the ITU's World Radiocommunication Conference (WRC), it was agreed that spectrum within the ultra high frequency (UHF) band, which has traditionally been the exclusive preserve of broadcasters, would be opened up for use by mobile internet broadband services.[50] This spectrum, commonly referred to as the digital dividend, is becoming available worldwide as a consequence of terrestrial television shifting from analogue to digital signals, which use considerably less bandwidth. It is highly sought after because of the quality of signal available and its propagation characteristics: the signals travel further and are more capable of penetrating buildings. The signal range means the cost of rolling out wireless broadband networks is considerably reduced, which is obviously beneficial for developing countries.[51]

Recommendations, Resolutions and Decisions

In addition to the binding legal instruments, the various bodies of the ITU adopt recommendations, resolutions, and decisions. Whilst the *Administrative Regulations* comprise the general principles to be complied with, the manner in which they are to be implemented are detailed in ITU-T and ITU-R Recommendations, which represent the bulk of ITU rule-making.[52] Such recommendations do not have 'the same legal status as the Regulations' (ITR 1988, Article 1.4), although 'administrations […] should comply with, to the greatest extent practicable, the relevant' recommendations (Article 1.6).[53] Draft recommendations are prepared within the various sectoral Study Groups and enter into force either through approval at the relevant assemblies or conferences, or through direct correspondence with Member State administrations (Convention, Articles 11(2), 14(1)).

In the event of a dispute regarding the interpretation of any of the legal instruments – Constitution, Convention or *Administrative Regulations* – settlement will either be achieved through mutually agreed bilateral or multilateral arrangements or, if not settled by such means, via an arbitration procedure (Constitution, Article 56). The decision of the arbitrator(s) shall be 'final and binding upon the parties to the dispute' (Convention, Article 41), although no enforcement mechanism is available in the event of non-compliance. A compulsory arbitration procedure is also provided for under an *Optional Protocol* to the Convention, between Members that are party to the Protocol.[54]

50 ITU Press Release, WRC-07, 'ITU World Radiocommunications Conference concludes after four weeks: International treaty sets future course for wireless', 16 November 2007.

51 Financial Times, 'Radio spectrum freed for mobiles', 19 November 2007.

52 Over 2600 ITU-T Recommendations are currently in force.

53 However, see also the opinion of the Advocate-General in *Italy v Commission* [1985] 2 CMLR 368, 373.

54 Constitution, Article 56(3).

Over recent years, numerous resolutions have been adopted by various ITU institutions and at conferences bestowing a mandate on the ITU and its sectors to address certain public policy matters relating to the internet and the management of its resources, from child online protection[55] to the deployment of Internet Protocol (IP) version 6 (IPv6).[56] As such, the ITU is just one of many international organisations with a remit to govern cyberspace (discussed further *infra* in section 5) and, while focusing primarily on technical network-related issues, its mandate extends to content-related matters as well.

4.2 World Trade Organisation

The WTO was established in 1994 as part of the final act embodying the results of the Uruguay Round of multilateral trade negotiations.[57] The function of the WTO is to facilitate the implementation, administration and operation of certain multilateral trade agreements.[58] A unique feature of the WTO system is the establishment of a Dispute Settlement Body to enforce the obligations accepted by Member States within the context of the agreements. The existence of an enforcement mechanism has been a key factor in pushing the WTO to the forefront of intergovernmental organisations.

For the telecommunications industry, the accelerating process of market liberalisation coincided with the *General Agreement on Tariffs and Trade* (GATT) Uruguay Round, which commenced in 1986. A key feature of the Uruguay Round was that for the first time trade in services was included within the scope of the multilateral negotiations. With the increasing importance of trade in services, particularly for developed nations, telecommunications was recognised as a critical element both as a facilitator of trade in services, and as an increasingly tradable service in its own right. Such recognition ensured that telecommunications issues moved towards the top of the agenda for countries such as the US and the UK.

At the conclusion of the Uruguay Round at Marrakesh in 1994, a series of trade agreements were adopted, of which only some are of relevance to the telecommunications sector. The GATT[59] is concerned with trade in goods and, as such, potentially impacts on trade in telecommunications equipment. In 1996, the major developed Member States adopted a further agreement within the context of GATT on Information Technology Products, which directly encompasses most forms of telecommunications equipment.

55 Resolution 179 (Guadalajara, 2010), 'ITU's role in child online protection', available at http://www.itu.int/osg/csd/intgov/resoultions_2010/PP-10/RESOLUTION_179.pdf.

56 WTSA, Dubai 2012, Resolution 64, 'IP address allocation and facilitating the transition to and deployment of IPv6', available at http://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2064.pdf.

57 See the *Agreement, Establishing the World Trade Organisation with Understanding on Rules and Procedures Governing the Settlement of Disputes and Trade Policy Review Mechanism* (Marrakesh, 15th April 1994; 33 ILM (1994)). The Treaty entered into force on 1 January 1995.

58 *Ibid*., at Article III(1).

59 33 ILM 28 (1994).

The *Agreement on Trade-Related Aspects of Intellectual Property* (TRIPS)[60] is also of obvious importance to an industry so heavily dependent on its investments in research and development. Other agreements which can and have impacted on the sector include the *Agreement on Subsidies and the Agreement on Government Procurement*.[61] However, this section focuses on the *General Agreement on Trade in Services* (GATS)[62] as the primary WTO-agreement establishing a framework for international telecommunications law.

4.2.1 General Agreement on Trade in Services

In terms of the scope of GATS, a Services Sectoral Classification List places Communications Services as the second category, which is then sub-divided into five sub-sectors: postal services, courier services, telecommunication services, audio-visual services, and other. Category C, Telecommunication Services, is further sub-divided into 15 sub-categories, including packet-switched data transmission services, which includes internet service provision. Those 15 services are further distinguished into basic and value-added services: 'all telecommunication services, both public and private that involve end-to-end transmission of customer supplier information for which suppliers "add value" to the customer's information by enhancing its form or content or by providing for its storage and retrieval.'[63]

Referring back to the earlier discussion about the scope of the regulated sphere, it is interesting to note that this definition views content manipulation as a means of adding value to a telecommunication service, rather than rendering the service as something other than a telecommunication service. Either way, the concept of value-added services would clearly encompass much that comprises communication services within the internet context.

The nature of telecommunication services means that they can be further distinguished into a number of categories on the basis of geographical scope (local, long-distance, and international); mode of transmission (wire and wireless or radio-based); the use and ownership of infrastructure (facilities-based or resale), and to whom the services are provided (public or non-public).[64] Some 108 Member States have made commitments to liberalise trade in telecommunication services.[65]

60 33 ILM 81 (1994).

61 For a complete list of WTO Legal Texts, see generally: http://www.wto.org/english/docs_e/legal_e/legal_e.htm.

62 33 I.L.M 44 (1994).

63 See http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_coverage_e.htm#basic.

64 *Ibid*.

65 See http://www.wto.int/english/tratop_e/serv_e/telecom_e/telecom_e.htm.

The GATS is concerned with four modes of supplying services:

i. from one territory to another, i.e. cross-border supplies;[66]
ii. the provision to foreign consumers in the service providers territory (i.e. consumption abroad);
iii. the establishment of a commercial presence in the another State; and
iv. through the presence of a natural person in another State.[67]

In terms of the telecommunications sector, modes (i) and (iii) are most relevant in terms of business practice.

The GATS contains an annex on telecommunications and, subsequently, a protocol establishing commitment in basic telecommunications. Taken together, these agreements have required Member signatories to substantially open up their telecommunication markets to international competition.

The GATS comprises a number of fundamental General Obligations and Disciplines to which all Members are required to comply from the moment the agreement entered into force (Part II). These general obligations are then supplemented by specific commitments accepted by a Member in a Schedule of Commitments appended to the GATS (Part III and IV). Each schedule specifies:

(a) terms, limitations and conditions on market access;
(b) conditions and qualifications on national treatment;
(c) undertakings relating to additional commitments;
(d) where appropriate, the time-frame for implementation of such commitments; and
(e) the date of entry into force of such commitments (Article XX).

These schedules represent a baseline or codification of conditions in a specific national market upon which a foreign service provider can rely. In addition, they constitute the starting-point for future negotiations to further liberalise the sector. A commitment may only be modified or withdrawn by a Member after three years from the date it entered into force (Article XXI).

The best known general obligation upon Members is the Most-Favoured-Nation (MFN) Treatment: '[...] each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like service and service suppliers of any other country' (Article II(1)). However, a Member may specify that this principle shall not be applicable to certain

66 This concept was examined in the *Telmex* case at para 7.25 *et seq.*

67 GATS, Article I(2).

measures listed in an Annex on Article II Exemptions.[68] Such MFN exemptions are subject to review after a five-year period, and should not exceed a period of ten years.[69]

Article VI of the GATS addresses domestic regulation. It requires Members to ensure that any authorisation procedures are handled 'within a reasonable period of time' (Article VI(3)) and are capable of 'objective and impartial review' by a judicial or administrative body (Article VI(2)). Such commitments are obviously applicable to licensing procedures for the provision of telecommunication services. In addition, there is an on-going commitment to develop disciplines to ensure that 'qualification requirements and procedures, technical standards and licensing requirements do not constitute unnecessary barriers to trade' (Article VI(4)).

Competition law issues are addressed under Part II, General Obligations and Disciplines, in Articles VIII (Monopolies and Exclusive Service Suppliers) and IX (Business Practices). Such rules may be used to prevent an abuse of dominant position or restrictive trade practices. These provisions can be seen as being of particular interest to telecommunication operators trying to provide services into countries whose legal systems have historically had no legal rules addressing general competition issues.[70]

In contrast to the GATT, the principle of national treatment constitutes a specific commitment applicable to particular service sectors as detailed in a Members' Schedule of Commitments to the GATS: '[...] each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of service, treatment no less favourable than that it accords to its own like services and service suppliers' (Article XVII).[71]

The other key specific commitment under the GATS concerns market access (Article XVI), under which Members detail those service sectors into which service suppliers from other Members may enter.

Telecommunications Annex

At the time of the GATS, Members also adopted a supplementary *Annex on Telecommunications*. Its objective was to clarify the position of Members 'with respect to measures affecting *access to and use of* public telecommunications transport networks and services' (paragraph 1). The Annex is therefore concerned with the supply of value-added telecommunication services over such public networks, such as internet access services, rather than any right to provide the underlying networks and services. These obligations are incurred, therefore, whether or not the Member has liberalised the provision of basic networks and services.

68 GATS, Article II(2).

69 GATS, Annex on Article II Exemptions, paras. 5–7.

70 E.g. Asian countries.

71 See GATT (1947), Article III, 'National Treatment on Internal Taxation and Regulation'.

The Annex imposes obligations of transparency of conditions of access and use, including tariffs, terms and conditions, and specifications of technical interfaces with the public networks and services (paragraph 4). The first draft of the Annex stated that access and use should be on cost-orientated terms, but this was removed in the face of opposition.[72] Access should be 'non-discriminatory', a term which embraces both the MFN and national treatment principles. Service providers should be permitted to attach terminal equipment to the public network, interconnect private circuits and use any operating protocols that do not interfere with the availability of the public network (paragraph 5(b)). In terms of restrictions, Members may only impose conditions that are necessary:

- to safeguard the public service responsibilities of the suppliers of public networks (i.e. the universal service obligation);
- to protect the integrity of the network; or
- to comply with a Member's commitments in its Schedule (paragraph 5(e)).

Such conditions may include restrictions on the resale of such services, compliance with any type-approval regime, or licensing and notification obligations. In addition, a developing country may impose conditions 'necessary to strengthen its domestic telecommunications infrastructure and service capacity and to increase its participation in international trade in telecommunications services' (paragraph 5(g)). To assist the growth of telecommunications in developing countries, developed Members are encouraged to make available information and opportunities concerning the transfer of telecommunications technology and training to the least-developed countries.

Fourth Protocol

At the conclusion of the Uruguay Round, ministers adopted a decision to enter into further voluntary negotiations on the liberalisation of trade for the provision of basic telecommunication networks and services.[73] These negotiations, carried out under the auspices of the Group on Basic Telecommunications, were scheduled to conclude no later than 30 April 1996. However there had been insufficient offers from Members to enable a conclusion to be reached by the deadline; therefore, negotiations were continued until an agreement was finally reached on 15 February 1997.[74]

This agreement is commonly referred to as the *Basic Agreement on Telecommunications*, although the term is somewhat misleading since the agreement consists primarily of a series of 'Schedules of Specific Commitments and a List of Exemptions from Article

72 Stated in Zutshi, B, 'GATS: Impact on developing countries and telecom services', p. 24, *Transnational Data and Communications Report*, July–August 1994.

73 33 ILM 144 (1994).

74 For a detailed history of the negotiations, see Sherman, L, '"Wildly Enthusiastic" about the first multilateral agreement on trade in telecommunications services', pp. 61–110, Federal Communications Law Journal, vol. 51, no. 1, 1999.

II concerning basic telecommunications' submitted by some 69 Members.[75] These commitments supplement or modify any existing submissions made by Members and are annexed to the existing schedules through a device referred to as a Protocol, which becomes an integral part of the GATS (Article XX). As such, these submissions constitute the *Fourth Protocol* to have been entered into by certain Members of the WTO. The *Fourth Protocol* was intended to enter into force on 1 January 1998; however, further delays meant that it became effective on 5 February 1998.

The Basic Agreement has been seen as the most significant development in the global liberalisation of the telecommunications market. It has been estimated that the Member countries represent over 90 per cent of global revenues in telecommunications.[76] The commitments made by Members encompassed market access, foreign direct investment and, for the majority of Members, adherence to a set of pro-competitive regulatory principles. The Protocol addressed the introduction of competition into the four biggest bottleneck markets within telecommunications: satellite services, international public voice telephony, domestic long distance, and the provision of the local loop.

Reference Paper

One unique feature of the *Fourth Protocol* was the adoption of a Reference Paper by 57 of the 69 Member signatories as an additional commitment incorporated into the Schedules.[77] The Reference Paper comprises a set of definitions and principles on the regulatory framework governing the provision of basic telecommunications. The principles address particular objectives for the establishment of a pro-competitive regulatory regime, rather than the mechanisms or processes for their achievement. As such, the Reference Paper represents an important body of international legal principles for the telecommunications sector, of considerably greater significance than the ITU constitutional principles. In addition, where a Member State has incorporated the Reference Paper into its Schedule of Commitments, the principles are enforceable before the WTO Dispute Settlement Body.

In terms of competition law, the Reference Paper firstly defines two key concepts, essential facilities and major suppliers. The concept of essential facilities originates in US antitrust law, although it has also been embraced within EU competition law.[78] The concept of a major supplier is similar to the traditional competition concept of dominance, and is similar to the current EU concept of an 'organization with significant

75 As of 25 October 2013, this number had risen to 99 members. See the WTO Secretariat compilation available at http://www.wto.org/english/tratop_e/serv_e/recap_e.xls.

76 See Spector, PL, 'The World Trade Organisation Agreement on Telecommunications', pp. 217–222, The International Lawyer, vol. 32, no. 2, Summer 1998.

77 This has since risen to 82 Member States.

78 For US law, see MCI Communications v AT&T, 708 F 2d 1081 (7th Cir 1983), 464 US 891 (1983); for EU law, see Case C-7/97 Oscar Bronner GmbH & Co KG v Mediaprint Zeitungs-und Zeitschriftenverlag GmbH & Co KG and Others [1998] ECR I-7791.

market power'. The perspective of the Reference Paper is the supplier's ability to affect access to the market by others, which reflects its international trade origins.

The first two substantive issues addressed in the Reference Paper concern controls to be placed upon the ability of a major supplier to be able to restrict competition. First, a supplier who, alone or with others, constitutes a major supplier must be subject to 'appropriate measures' to prevent anti-competitive practices, whether current or future. Three specific anti-competitive practices are then listed:

- cross-subsidisation;
- the use of 'information obtained from competitors with anti-competitive results', such as the forecast traffic volumes in interconnection arrangements; and
- 'not making available to other services suppliers on a timely basis technical information about essential facilities and commercially relevant information which are necessary for them to provide services' (paragraph 1.2).

Second, interconnection with a major supplier should be 'ensured at any technically feasible point in the network'. Such interconnection should be on non-discriminatory terms and conditions, on the basis that such terms and conditions should be no less favourable than those provided for its own like services, echoing the national treatment principle under the GATS. The interconnection must be achieved in a timely fashion and on 'cost-oriented rates that are transparent, reasonable, having regard to economic feasibility, and sufficiently unbundled so that the supplier need not pay for network components or facilities that it does not require for the service to be provided'. Interpretation of this critical concept of cost-orientation is already the subject of international dispute. Finally, the request for interconnection may be in respect of network termination points which are not offered to the majority of users.

Building on the *Annex on Telecommunications*, the procedures and arrangements for interconnection with a major supplier must be transparent, including publication of 'either its interconnection agreements or a reference interconnection offer'. A service supplier must have recourse to an independent domestic body to resolve any disputes that may arise in respect of interconnection.

The other four issues covered in the Reference Paper address broader aspects of a pro-competitive telecommunications market:

- defining a 'universal service obligation' will 'not be regarded as anti-competitive *per se*', provided they are addressed in a transparent and non-discriminatory manner and are necessary to achieve the universal service defined by the Member State (paragraph 3);
- reflecting Article VI of the GATS, any licensing criteria must be publicly available, as well as 'the terms and conditions of individual licences'; and the reasons for any licence denial must be made known to the applicant (paragraph 4);

- although the need for, and form of, any regulator is not addressed, the Reference Paper imposes an obligation upon a Member State to ensure that any such regulator(s) are 'separate from, and not accountable to, any supplier of basic telecommunications services' (paragraph 5); and
- the allocation and use of scarce resources, 'including frequencies, numbers and rights of way', should be carried out in an objective, timely, transparent, and non-discriminatory way (paragraph 6).

Whilst the Reference Paper addresses 'ends' rather than 'means', its influence is considerable at both a national and international level. First, as part of the Schedules of Commitments, the Reference Paper represents a Member State's commitment to which foreign service providers may refer. Second, over time national legislators are likely to reflect and incorporate such principles into domestic law. Third, the Reference Paper represents a baseline from which any future multilateral negotiations will depart.

The Reference Paper, as a unique set of international legal principles for the telecommunications sector, is not only pro-competitive, but would also seem sufficiently detailed to constitute possible grounds upon which to instigate legal proceedings in the event that a Member State failed to comply. However, this begs the question of the status of the WTO agreements in the legal systems of those some 60 nations that have incorporated it into their 'Schedule of Commitments'. This issue can be divided into two questions:

- whether the WTO agreements, and in particular the Reference Paper, may be used in the interpretation and application of national or regional (e.g. EU) telecommunications regulations; and
- whether the Reference Paper could be used as the basis for initiating proceedings before a court in the event of a conflict with existing regulations, i.e. have direct effect.

In the absence of direct effect, under either regional or national law, the only mechanism under which a party could seek enforcement against a Member State for failure to comply with their obligations in respect of the telecommunications sector is through the WTO Dispute Settlement Body.

4.2.2 Dispute Resolution

A unique feature of the multinational trade negotiations concluded in 1994 was the establishment of a dispute settlement mechanism applicable to trade agreements.[79] For the first time, disputes between Member governments about compliance with an international treaty can be submitted to an independent body, the Dispute Settlement

[79] See generally, Merrills, J.G. *International Dispute Settlement* (5th ed.), Cambridge University Press, 2011.

Body (DSB), and a defaulting party may be made subject to enforcement procedures.[80] The *Understanding on rules and procedures governing the settlement of disputes* (Understanding) encompasses the GATS and therefore is applicable to disputes concerning commitments made in respect of national telecommunications markets.[81]

Under the agreed procedures, a Member government may request the establishment of a Panel by the DSB. However, it would not seem appropriate to characterise the DSB as a judicial body. The Panel comprises three individuals chosen by the DSB secretariat with the consent of the parties. In the absence of agreement, the Director-General may appoint the panellists. After an investigation, the Panel submits a report to the DSB for consideration, detailing its findings and conclusions. The DSB will usually adopt the Panel report, unless one of the parties notifies the DSB of its intention to lodge an appeal to the Appellate Body (Article 17). The Panel or Appellate Body will decide whether a particular Member State's measure is inconsistent with the terms of the relevant agreement, and may recommend ways of overcoming the issue. A Member against whom a decision has been reached is obliged to implement the recommendations and rulings of the DSB within a reasonable period of time (Article 21).

In the event that a Member fails to comply, the Understanding allows for the payment of compensation or the suspension of concessions (Article 22). The ability to suspend trade concessions granted to an infringing Member is the real stick within the dispute settlement procedure under the WTO. A complaining party may be able to suspend concessions or obligations not only in the sector of dispute (e.g. telecommunications), but also, where appropriate, in other sectors under the same agreement (e.g. GATS), or even under another covered agreement. Any such concession must be authorised by the DSB and should be 'equivalent to the level of the nullification or impairment' (Article 22.4).

Whilst the WTO dispute procedures are between governments, industry obviously plays an important role in bringing such matters to their attention. Under European law, complaints may be submitted in writing to the EU Commission, and a formal examination procedure may be invoked prior to the decision to pursue a dispute.[82] In the US, the Office of the United States Trade Representative is required to annually solicit comments from industry on the implementation of the 'Basic Agreement' pursuant to the *Omnibus Trade and Competitiveness Act* of 1988.[83]

---

80 The dispute settlement system under GATT 1947 was essentially a conciliation procedure.

81 *Understanding on rules and procedures governing the settlement of disputes* (Annex 2 to the WTO Agreement), at Appendix 1.

82 See Council Regulation (EC) No. 3286/94 of 22 December 1994 laying down Community procedures in the field of the common commercial policy in order to ensure the exercise of the Community's rights under international trade rules, in particular those established under the auspices of the World Trade Organisation; OJ L 349/71, 31.12.1994.

83 19 USC s 1377. A determination that a foreign country is either not in compliance with a telecommunications-related agreement is treated as a violation of a trade agreement under the *Trade Act* of 1974, s 304(a)(1)(A),

The dispute settlement procedures have so far been invoked in respect to very few disputes in the telecommunications sector. Formal proceedings before the DSB have been pursued by the European Commission against Korea[84] and Japan in respect of preferential trade practices in favour of US suppliers of telecommunications equipment, both of which were resolved by agreement.[85] Proceedings have also been brought by the US against Belgium, regarding telephone directory services,[86] which was settled. The only case to reach a Dispute Panel and a formal decision was a claim made by the US against Mexico, the so-called 'Telmex case'.[87]

In the vast majority of situations it is the threat of WTO proceedings that is used as a stick to encourage resolution through negotiation. The US has been particularly willing to issue such threats, such as against Canada, regarding discrimination against US-based carriers transmitting international traffic,[88] and Germany, regarding Deutsche Telekom's failure to meet interconnection obligations and discrimination against foreign carriers for call completion.[89]

4.2.3 The Doha Round

The process of trade liberalisation under the WTO regime is on-going, with multinational negotiations attempting to broaden and deepen the commitment of Member States to free trade. The current round of negotiations formally commenced at Doha, Qatar, in November 2001.[90] In parallel with these negotiations, Member States are negotiating and entering into bilateral trade agreements with trading partners; these agreements usually go beyond what are prepared to commit at a multinational level. Telecommunications forms a component of the current round, with the major industrialised countries calling upon other countries to make commitments to fully liberalise, and the 'elimination of MFN exemptions for telecommunication services'.[91] Other than such calls for adoption, however, there is little by way of substantive proposals to amend the existing agreements, which is illustrative of how far and how successful the current agreements have been in terms of fundamentally changing national and international telecommunications law.

---

19 USC §2101.

84 WT/DS40 'Korea—Laws, regulations and practices in the telecommunications procurement sector', 5 May 1996.

85 WT/DS15 'Japan—Measures affecting the purchase of telecommunications equipment', 18 August 1995.

86 WT/DS80 'Belgium—Measure affecting commercial telephone directory services', 13 May 1997.

87 See 'Mexico—Measures affecting Telecommunication Services', Report of the Panel, WT/DS204/R, 2 April 2004.

88 See 1998 Annual Report of the President of the United States on the Trade Agreements Program, at p. 257.

89 See 'US warns on German telecoms', Financial Times, 12 August 1999. See also 1999 Annual Report, at p. 293.

90 WTO Ministerial Declaration, 14 November 2001 (WT/MIN(01)/DEC/1).

91 TN/S/W/50, 'Communications from Australia, Canada, the European Communities, Japan, Hong Kong China, Korea, Norway, Singapore, the Separate Customs Territory of Taiwan, Penghu, Kinmen, and Matsu and the United States', 1 July 2005.

5. Internet Governance

As the phrase 'internet governance' has gained widespread usage in relation to cyberspace policy, its meaning has become more diffuse.[92] 'Governance' is widely used to embrace a wide range of different management and control mechanisms, of which traditional laws and regulations form only one segment. Other sources of governance include technical and operational standards and protocols developed in formal and less formal fora, such as the ITU and the Internet Engineering Task Force. The role standards and other technical decision-making play in determining the regulation of cyberspace has been examined extensively elsewhere.[93] For the purposes of this section, it is important to examine how the on-going debates about the future of internet governance impinge on the areas of international telecommunications law examined in the chapter.

From a telecommunications perspective, the internet as a network of networks is subject to a multitude of national, regional and international laws and regulations that together can be said to govern it. Each network and service provider is required to comply with the national rules applicable to it by virtue of the jurisdictional reach that each law claims, whether based on the presence of physical infrastructure, the exercise of managerial control or simple consumption by end-users. The WTO may have liberalised cross-border trade in telecommunications, but it does not prohibit the recipient State from regulating the conditions of supply by a service provider. Indeed, even in Europe, the provision of telecommunications is not subject to the 'country of origin' principle applicable to other internet-related services, such as information society services and audiovisual media services,[94] which would require a provider to comply only with the rules of its home jurisdiction when providing services to the other 27 Member States. Similarly, US operators are subject to both federal and State regulation.[95] As such, internet governance could be viewed as the totality of all these distinct national and regional rules and regulations governing the provision of these networks and services.

Within that array of laws, the provision of numbering is a key resource. Numbering systems can identify the sender or recipient of a communication, the route or service by which a communication is transmitted, or the network and service providers involved in a transmission. Similar to spectrum, numbering schemes are seen as requiring management in order to ensure that harmful interference does not occur, in the sense that the same number is not used by multiple parties, preventing effective communication.

---

92 Bygrave, L., and J. Bing, Internet Governance: Infrastructure and Institutions, OUP, 2009.

93 See Lessig, L, *Code and Other Laws of Cyberspace*, Basic Books, 2000 and Reidenberg, JR, 'Lex informatica: The formulation of information policy rules through technology', 76 *Texas Law Review* 553, 1998.

94 See Directive 2000/31/EC 'on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market' (OJ L 178/1, 17.7.2000) and Directive 2010/13/EU 'on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services' (OJ L 95/1, 14.4.2010).

95 E.g. the Federal Communications Commission and the various State Public Utility Commissions.

Numbering regimes operate at a national, regional and international level, such as the ITU's Recommendation E.164, which implements an international numbering plan for public telecommunications.[96]

With the emergence of the internet, a new naming and addressing scheme was established, the Internet Protocol (IP) address and the domain name system. While this new scheme adopted international standards, such as the two letter codes designating different countries[97] such 'uk' and 'fr', because cyberspace was effectively 'born global', from the start it also contained generic Top-Level Domains, such as 'com' and 'net', which effectively circumvented national numbering regulations. As such, the management of the IP and domain name system is often seen as the nearest thing we have to a central governance regime for cyberspace. Over time elements of the system have been brought within the effective jurisdiction and management of national[98] and regional[99] regimes, but it is still primarily controlled at a global level.

The IP addressing and domain name system is managed by the Internet Assigned Number Authority (IANA), which is part of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is currently a 'nonprofit public benefit corporation' under Californian law, operating under contract to the US Department of Commerce in respect of the management of the IANA function. As such, the US is viewed as having effective control over the governance of the internet, which raises obvious concerns for some jurisdictions.

One element of the debates over internet governance has revolved around the issue of whether control of the domain name system and related IP numbers should be transferred to another body such as the ITU. In addition to amending the ITRs, the parties at ITU's WCIT 2012 also adopted a number of Resolutions, one of which directly addressed internet governance issues and, as a consequence, proved highly controversial. The Resolution stated the following: '[...] all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future internet [...]'.[100]

---

96 Available at http://www.itu.int/rec/T-REC-E.164-201011-I/en.

97 International Standards Organization (ISO) Standard 3166-1: 2006.

98 Under UK law, for example, while the concept of a 'number' is widely defined to include 'data of any description' (*Communications Act* 2003, s. 56(10)), internet domain name and addresses have subsequently been excluded from the national regulatory regime (*The Telephone Number Exclusion (Domain Names and Internet Addresses) Order* 2003).

99 Regulation No. 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain (OJ L 113/1, 30.4.2002) and Commission Regulation (EC) No. 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (OJ L 162/40, 30.4.2004).

100 Resolution 3, 'To foster an enabling environment for the greater growth of the Internet', at para. e).

This was seen as a challenge to the *status quo*, especially regarding the governance of ICANN and an extension of the ITU's mandate. However, beyond the ITU, there are increasing demands for a change in the manner of governance. In October 2013, for example, the leading organisations responsible for the internet's technical architecture[101] issued a statement calling for the globalisation of the ICANN and IANA functions, 'in which all stakeholders, including all governments, participate on an equal footing'.[102]

Obviously, the ITU cannot be seen as necessarily neutral in such debates, since it would inevitably enhance its status to be given such responsibilities. Those against consider that a shift to the ITU, with its 'one State one vote' decision-making processes and inevitable developing nation majority, would place too much control in the hands of governments that may adopt a less liberal approach to the operation of the internet. However, recent revelations by Edward Snowden about the US National Security Agency's widespread surveillance of internet traffic have raised serious questions about the extent to which the US is in fact a suitable controlling entity.

6. Concluding Remarks

This chapter has examined international telecommunications law through the lens of two intergovernmental institutions, the ITU and the WTO, and their respective legal instruments. The activities of the former more directly govern aspects of the internet, as the network of networks, including standard-setting and the availability of spectrum for wireless broadband. With the controversial amendments to the ITRs and its other activities in areas such as cybersecurity, the ITU is also moving towards a more direct involvement in the regulation of cyberspace.

The WTO agreements have had a less direct impact on the internet, being primarily concerned with ensuring a regulatory environment that stimulates and facilitates the competitive provision of telecommunications networks and services, which is both a reflection of the growth of the internet and an influence on its future development. With respect to cyberspace, the WTO currently has little influence, and the latest round of trade negotiations is progressing very slowly.

International telecommunications law is simply one relatively uncontroversial strand of an increasingly complex governance framework for the internet and cyberspace. This framework is likely to become more diffuse and entangled as the internet evolves and matures over the coming decades.

101 Including ICANN, Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), Internet Society (ISOC) and World Wide Web Consortium (W3C).

102 Montevideo Statement on the Future of Internet Cooperation (7 October 2013), available at http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm.

Wolff Heintschel von Heinegg

Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law

1. Introduction

'International cyber security law' is far from being a self-contained, established and highly-developed legal regime. The term 'international cyber security law' is but a label for a legal cross-sectional area, consisting of a panoply of rules and principles derived from most diverse subject areas of international law, whose principal applicability to cyberspace and whose concurrence have not yet been fully analysed. It is, therefore, necessary to closely analyse those branches of international law that are, or may be, of relevance for the security and stability of the global information and communications infrastructure.

As far as the international law of the sea is concerned, its provisions are of relevance for activities in cyberspace that take place at or via the sea, and in or through the airspace above the various sea areas. Hence, during innocent passage through the territorial sea, ships may not engage in cyber operations that would be 'prejudicial to the peace, good order or security of the coastal State.'[1] Similar, though less strict, prohibitions apply to ships and aircraft in transit passage or in archipelagic sea lanes passage.[2] In the other sea areas, ships and aircraft are obliged to comply with the general obligation to refrain from an unlawful use or threat of force, and to pay due regard to the legitimate interests of other States.[3] The fact that warships and other State ships enjoy sovereign immunity[4] does not relieve them from these well-established obligations.

The present chapter deals with one aspect of the international law of the sea that may be considered as vital for cyberspace security – the international legal protection of submarine communications cables.[5] Its focus is on the peacetime rules of the law of the

1 *United Nations Convention on the Law of the Sea* of 10 December 1982, Article 19(1), 1833 UNTS 3, entry into force on 16 November 1994 (in the following referred to as '1982 LOSC' or 'LOSC'). For activities that qualify as 'prejudicial' see, in particular, Article 19(2)(a) to (d). These prohibitions, according to Articles 45 and 54, also apply to the exercise of the right of innocent passage through international straits and archipelagic waters. It may be added that, according to Article 20, 'submarines and other underwater vehicles are required to navigate on the surface and to show their flag.'

2 Articles 39, 40 and 53 LOSC.

3 Articles 58(3), 87(2), 88 and 301 LOSC.

4 Articles 32, 95 and 96 LOSC.

5 Submarine communications cables must be distinguished from other submarine cables, in particular from 'high-voltage cables' and from cables used for disaster preparedness. For a description of the characteristics of submarine communications cables see M. Sechrist, *Cyberspace in Deep Water: Protecting Undersea*

sea. The legal status of submarine communications cables in times of an international armed conflict is not dealt with here.[6]

2. Significance and Vulnerability of Submarine Communications Cables

2.1 Significance

Since the second half of the 19th century, submarine cables have been used for international communications. In the beginning, transatlantic cables were used for telegraph communications, with the first transatlantic telegraph cable being laid in 1866.[7] In the 1950s, submarine cables became increasingly important for transoceanic telephone communications,[8] and as of today, about 300 submarine cables have been laid. They directly connect more than 130 States and they have become the backbone for international telecommunications and data traffic.[9] With the introduction of fibre-optic cables (since the 1980s), the capacities of submarine cables have increased considerably. Today, a single cable can carry millions of telephone calls, together with huge amounts of video and internet data.[10] Submarine cables 'carry over 95% of the world's international voice, data, and video traffic, including almost 100% of transoceanic Internet ocean traffic'[11] and, because of their bandwidth, the 'lower cost and longer lifespan [they] have surpassed satellites as the principal means of delivering

Communication Cables By Creating an International Public-Private Partnership (Harvard Kennedy School, 23 March 2010), available at: http://belfercenter.hks.harvard.edu/files/PAE_final_draft_-_043010.pdf (last visited on 19 August 2013).

6 Under the law of international armed conflict, submarine cables are only protected if they connect an occupied territory with a neutral territory. Even then, they may be seized or destroyed in cases of 'absolute necessity'. See Article 54 of the 1907 *Hague Regulations Respecting the Laws and Customs of War on Land*. See also C.J. Colombos, *The International Law of the Sea*, at p. 535 *et seq*. (6th ed., Longman 1967); A. Pearce Higgins, 'Submarine Cables and International Law', 2 BYIL pp. 27-36 (1921-1922); *Tallinn Manual on the International Law Applicable to Cyber Warfare*, at p. 247, pp. 250 *et seq*. (ed. by Michael N. Schmitt, Cambridge University Press 2013).

7 The first submarine cable was laid between Dover and Calais in 1851, see Colombos, *ibid*., at p. 381.

8 S. Coffen-Smout / G.J. Herbert, 'Submarine Cables: A Challenge for Ocean Management', 24 Marine Policy pp. 441-448, at p. 441 *et seq*. (2000). See also S. Gordon, *A Thread Across the Ocean*, *passim* (2002).

9 See the interactive map available at: http://www.telegeography.com/telecom-resources/submarine-cable-map/index.html (last visited on 14 August 2013).

10 See International Cable Protection Committee (ICPC), *About Submarine Telecommunication Cables 2011*, available at: http://iscpc.org/publications/About_SubTel_Cables_2011.pdf (last visited on 19 August 2013).

11 L. Carter / D. Burnett / S. Drew / G. Marle / L. Hagadorn / D. Bartlett-McNeill / N. Irvine, *Submarine Cables and the Oceans: Connecting the World*, at 8 (UNEP-WCMC Biodiversity Series No. 31, ICPC / UNEP-WCMC (2009), available at: http://www.unep-wcmc.org/medialibrary/2010/09/10/352bd1d8/ICPC_UNEP_Cables.pdf (last visited on 19 August 2013); L.R. Wrathall, 'The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward', 12 San Diego Int'l L.J. pp. 223-261, at p. 228 (2010-2011). See also E.J. Malecki / Hu Wei, 'A Wired World: The Evolving Geography of Submarine Cables and the Shift to Asia', 99 Annals of the Association of American Geographers pp. 360-382, at p. 362 (2009); M.P. Green / D.R. Burnett, 'Security of International Submarine Cable Infrastructure – Time to Rethink?', in: *Legal Challenges in Maritime Security*, pp.557-583, at p. 559 (M.H. Nordquist et al. eds., M. Nijhoff 2008).

international telecommunications traffic.'[12] According to other sources, '99 percent of the world's long-distance communications travel through fibre links. The remaining 1 percent are […] satellite-based.'[13] It may be added that 'even communication networks that start with satellite systems (such as ships at sea) often are dependent on seabed cables to connect satellite ground stations with end users.'[14] Although used for commercial and governmental purposes, most of these cables and cable networks are owned and operated by consortia of private carriers.[15] Many contemporary security and military operations, in particular the use of unmanned aerial systems, depend upon global network reliability. The necessary bandwidth can only be provided by submarine cables that 'provide fast, large and inexpensive connection.'[16]

2.2 Threats to Submarine Cables

Due to the characteristics of the environment in which they are laid, submarine cables have always been exposed to a variety of natural and man-made threats. However, with the introduction of fibre-optic cables and the ensuing dependence of businesses and governments on trans-ocean communications, the 'world's oceans have become a target-rich environment that provides adversaries with incentives to develop undersea operational competence and strike these difficult-to-defend systems.'[17]

An interruption of the flow of data through submarine cables causes a loss of connectivity that may bring to a halt important military operations as well as government and commercial communications, in particular financial transactions.[18] According to Douglas Burnett, 'service interruptions of these high-bandwidth fibre optic communications systems can result in excess of $1.5 million revenue loss per hour.'[19]

---

12 Wrathall, *ibid*. See also Coffen-Smout / Herbert (*supra* note 8), at p. 441.

13 Sechrist (*supra* note 5), at p. 16, citing Jim Hayes, President of the California-based Fiber Optic Association.

14 K.M. Hasslinger, 'Undersea Warfare: the Hidden Threat', Armed Forces Journal (1 March 2008), available at: http://armedforcesjournal.com/article/2008/03/3348196 (last visited on 19 August 2013).

15 For instance, the US Defense Information Systems Agency (DISA) 'relies on commercial networks for 95 percent of the infrastructure [used] for strategic communications.' See Sechrist (*supra* note 5), at p. 9. See also *ibid*., at p. 17, quoting the Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs that stated, 'the private sector owns the preponderance of [US] critical infrastructure – estimates range from 85 percent to 95 percent.' Sechrist believes 'for undersea cables, the figure is closer to 100%.'

16 Sechrist, *ibid*., at p. 10.

17 Hasslinger (*supra* note 14).

18 For instance, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) uses submarine fibre-optic cables to transmit financial assets between almost all States in the world.

19 D. Burnett, 'Submarine Cable Infrastructure Defense Against Terrorists', Sea Technology Magazine (July 2005). Sechrist (*supra* note 5, at p. 18) adds that this 'estimate deals strictly with the costs for cable operators; it does not deal with the revenue lost for those whose traffic goes down on that cable system. In that respect, as well as the fact the estimate is five years old, it can be considered quite low.'

Still, the loss of connectivity through a single submarine cable will, in most instances, have but a minor impact on global communications because, as often service can be rerouted through other cables, and because broken cables can be repaired comparatively speedily. It must be borne in mind, however, that not all cable operators provide for additional capacities. Many countries do not have the funds necessary to support multiple cable landing stations or routes. Therefore, 'countries like India, Pakistan, Egypt, Vietnam, Maldives, Qatar, Taiwan and several in West Africa have lost over 80% capacity' between 2005 and 2010.[20] With the introduction of fibre-optic cables, 'a large percentage of overall bandwidth' has been concentrated 'in a few major cable systems' and 'cables come ashore in only a few places.'[21] Hence, interference with a single cable or with one of its landing points can have far-reaching effects in other regions as well. Moreover, 'multi-cable outages can occur and severely hamper day-to-day operations.'[22]

Submarine cables are either laid on the seabed or they are buried in the subsoil thereof. Apart from natural disasters,[23] the most common threat posed to unburied submarine cables are ships' anchors that are often dragged for long distances thus catching cables and bending them beyond a workable point. Bottom trawling by fishing vessels and clam dredgers may cause similar damage.[24]

Such interference will, in most cases, be the result of ignorance or negligence. In recent years, however, cable theft has proven to constitute yet another significant threat to submarine cables. A well-known incident occurred in 2007, when the Thailand-Vietnam-Hong Kong system (TVH) was interrupted at two, widely separated locations. At 'one location, 98 km of cable and one optical amplifier belonging to TVH had been stolen. At the second location, 79 km of cable and another optical amplifier belonging to APCN [Asian Pacific Cable Network] had been stolen.'[25] The substantial damage to the systems had been caused by Vietnamese vessels. Allegedly, the Vietnamese fishermen had misunderstood (or misinterpreted to their advantage) an agreement allowing them to salvage aging undersea copper cables. However, there were also reports suggesting that the depredations were attributable to the Vietnamese Government or that it 'failed to exercise due diligence in supervising the activities of its registered vessels which were acting pursuant to a 2006 agreement with the State, in not arresting the culprit vessels and not taking timely effective measures to prevent their continued operation and in

20 Sechrist (*supra* note 5), at p. 36.

21 Hasslinger (*supra* note 14).

22 Sechrist (*supra* note 5), at p. 20.

23 See Sechrist, *ibid*. at p. 18, referring to the 2006 earthquake off the coast of Taiwan.

24 Y. Takei, *Law and Policy for International Submarine Cables in the Asia-Pacific Region*, at p. 3, Asian Society of International Law, Working Paper 2010/13 (2011), available at: http://asiansil.org/publications/2010-13%20-%20Yoshinobu%20Takei.pdf (last visited on 19 August 2013). See also the list of significant cable breaks since 2003 provided by Sechrist (*supra* note 5), at pp. 38 *et seq*.

25 Green / Burnett (*supra* note 11), at p. 559.

allowing the vessels to continue to operate from Vietnamese ports.'[26] Other incidents of cable theft occurred in Jamaica (2008) and in South Africa (2008).[27]

Submarine cables may also be intentionally damaged, either by criminals or by terrorists and even State actors.[28] In Bangladesh and in California, cables were damaged by man-made cuts. Allegedly, there was a case in Spain in which a system was badly damaged by a bomb planted in the terminal station.[29]

So far, submarine cables have not been damaged or destroyed at sea by State actors or by terrorists. It would be naïve, however, to believe that they will not 'become the focal point of future nation-state conflicts, as well as prime targets for global insurgencies.'[30] Small submarines and unmanned underwater systems have become increasingly affordable and are no longer in the exclusive use of navies or other State agencies. They could, indeed, be 'used to deliver threatening payloads or to disrupt seabed infrastructure.'[31] At first glance, it may appear to be easier for malicious State and non-State actors to attack the landing point of submarine cables. However, there is a high probability of attacks from under the sea because detection is a rather difficult task (stealth), because they imply the advantages of surprise and of economy of force, and because they can circumvent defensive measures. 'A final incentive is the imposition of a cost-imposing strategy.'[32]

Finally, cable espionage has since long been an integral part of military operations. Already in the 1970s, the United States (US) Navy very successfully spied on Soviet cables (Operation Ivy Bells).[33] Today, the US Navy – and certainly other navies as well – is able to intercept the data traffic routed through submarine fibre-optic cables. An example is the USS *Jimmy Carter* that was put into service in 2005. According to reports, this nuclear-powered submarine has the 'ability to eavesdrop on communications – what the military calls signal intelligence – passed through the airwaves […]. But its ability to tap undersea fibre-optic cables may be unique in the fleet.'[34] The report continues:

> 'The capacity of fibre optics is so much greater than other communications media or technologies, and it's also immune to the stick-up-an-antenna type of

26 *Ibid*., at p. 565, p. 567.

27 Sechrist (*supra* note 5), at p. 40.

28 See The President's National Security Telecommunications Advisory Committee (NSTAC), *Report to the President on International Communications* (NSTAC, 16 August 2007).

29 Sechrist (*supra* note 5), at p. 51.

30 Hasslinger (*supra* note 14).

31 *Ibid*.

32 *Ibid*.

33 Sechrist (*supra* note 5), at p. 51.

34 'New Nuclear Sub Is Said to Have Special Eavesdropping Ability', *New York Times* of 20 February 2005, available at: http://www.nytimes.com/2005/02/20/politics/20submarine.html?_r=0 (last visited on 19 August 2013).

> eavesdropping,' said Jeffrey Richelson, an expert on intelligence technologies. To listen to fiber-optic transmissions, intelligence operatives must physically place a tap somewhere along the route. If the stations that receive and transmit the communications along the lines are on foreign soil or otherwise inaccessible, tapping the line is the only way to eavesdrop on it. The intelligence experts admit there is much that is open to speculation, such as how the information recorded at a fiber-optic tap would get to analysts at the National Security Agency for review.[35]

According to other reports, transmission to the National Security Agency is accomplished by attaching a splitter to the cable that is connected to a separate cable.[36] Allegedly, the submarine also intercepts fibre-optic light waves by slightly bending the cable. The quantity of escaping light is minor but sufficient to monitor the data traffic through the cable. Then the data from the transmissions are stored aboard.

It is quite probable that navies also have the capability to conduct cyber attacks through submarine cables and to use such cables for a variety of other military and operational purposes.

3. The International Legal Regime of Submarine Cables

In view of their importance for international communications, it is not surprising that, after the first transatlantic cable had been laid, States comparatively quickly agreed on treaty rules aimed at the protection of submarine cables. Of course, the first treaty rules were limited to 'submarine telegraph cables'.[37] Later, the scope of applicability was extended to cables used for 'telephonic communications' and to 'high voltage power cables'.[38] It has been doubted whether fibre-optic cables are also governed by the existing legal regime on submarine cables because they are not explicitly mentioned in the relevant treaty provisions.[39] Indeed, in 1884 and in 1958, fibre-optic cables were not envisioned. The same probably holds true for the delegations to the Third United Nations Conference on the Law of the Sea that finalised its work in 1982, i.e. shortly before fibre optic cables were actually used. An interpretation of the treaty provisions exclusively based on the wording would be overly formalistic. First, the provisions, in particular the 1982 LOSC, only partly distinguish between 'telegraphic', 'telephonic',

35 *Ibid*.

36 See Christoph Sydow, 'NSA-Abhörskandal: Die Datenräuber von der USS "Jimmy Carter"', Spiegel Online of 1 July 2013, available at: http://www.spiegel.de/politik/ausland/die-uss-jimmy-carter-soll-fuer-die-nsa-glasfaserkabel-anzapfen-a-908815.html (last visited on 19 August 2013).

37 *Convention for the Protection of Submarine Telegraph Cables*, Paris, 14 March 1884, 18 USTS 380, 75 BFSP 356.

38 *Geneva Convention on the High Seas* of 29 April 1958, Article 27, 450 UNTS 82; Article 113 LOSC. For the legal regime on high voltage cables see R. Lagoni, *Legal Aspects of Submarine High Voltage Direct Current (HVDC) Cables*, at 10 *et seq*., 41 *et seq*. (LIT 1999).

39 Takei (*supra* note 24), at p. 10.

and 'high voltage' cables in the context of the obligation relating to the punishment for breaking cables. Other provisions generally deal with 'submarine cables'. Hence, it is safe to conclude that all submarine cables are governed by those provisions irrespective of their design and function. Second, even those provisions explicitly dealing only with certain submarine cables have to be interpreted in the light of the subsequent practice of the States party to the respective treaties. That practice is sufficiently indicative of a generally shared position, according to which, fibre-optic cables and 'telegraphic', 'telephonic', and 'high voltage' cables are governed by the same rules.[40]

3.1 The 1884 Convention

After the laying of the first transatlantic cable in 1866,[41] States realised the value of submarine cables and the necessity for their protection against wilful or culpably negligent interruption or obstruction in sea areas beyond their national jurisdiction. Consequently, in 1884, 30 States adopted the *Convention for the Protection of Submarine Telegraph Cables* (1884 Convention).[42] It only regulates interference with telegraph cables, not with the freedom of laying them.[43] Today, the Convention is in force for 41 States and it may be considered as reflecting the customary international law on the matter. Although the International Law Commission (ILC), when preparing the draft *Articles concerning the Law of the Sea,*[44] only in part relied upon the 1884 Convention, it is safe to submit that the 'provisions of [the Convention] have been generally accepted as customary international law.'[45] Those who question the fundamentally norm-creating character of the 1884 Convention and who maintain that the small number of States Parties is indicative of a lack of a general practice,[46] forget that it still constitutes the international legal basis for domestic legislation for the protection of submarine cables, including States that have become parties to the 1982 LOSC.

---

40 See S.N. Nandan / S. Rosenne (eds.), *United Nations Convention on the Law of the Sea 1982: A Commentary*, Vol. III, at p. 270 (M. Nijhoff 1995).

41 *Supra* note 7.

42 *Supra* note 37.

43 D.P. O'Connell, *The International Law of the Sea*, Vol. I, at p. 508 (ed. by I.A. Shearer, The Clarendon Press 1982).

44 International Law Commission, *Articles concerning the Law of the Sea with commentaries*, YBILC 256 *et seq.* (1956 II).

45 American Law Institute, *Restatement of the Law Third, The Foreign Relations of the United States* Vol. 2, § 521, at p. 80 (1987). See also E. Wagner, 'Submarine Cables and Protections Provided by the Law of the Sea', 19 Marine Policy pp. 127-136, at p. 134 (1995). For the position according to which the provisions of the 1884 Convention, which have not been incorporated into the 1982 LOSC, do not reflect customary international law, see R. Beckman, 'Submarine Cables – A Critically Important but Neglected Area of the Law of the Sea', at pp. 16 *et seq*., Paper presented at Indian Society of International Law, 7th International Conference on Legal Regimes of Sea, Air, Space and Antarctica, New Delhi, January 15-17, available at: http://cil.nus.edu.sg/wp/wp-content/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables-rev-8-Jan-10.pdf (last visited on 19 August 2013).

46 Beckman, *ibid*., at p. 3.

According to its Article I, the 1884 Convention applies 'outside territorial waters to all legally established submarine cables landed on the territories, colonies or possessions of one or more of the High Contracting Parties.' Thus, submarine telegraph cables connecting one or more of the States Parties are included into the Convention's protective scope that is, however, limited to times of peace.[47] Under Article II (1), it is 'a punishable offence to break or injure a submarine cable, wilfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communication, either wholly or partly, such punishment being without prejudice to any civil action for damage.'[48] The exercise of criminal jurisdiction for interference with submarine telegraph cables is limited to the flag State of the vessel 'on board of which the offence was committed' – Article VIII (1) – or to the State of nationality of the perpetrator – Article VIII (2). Hence, the States Parties did not consider the breaking of a submarine telegraph cable to constitute an act of piracy.[49] Other provisions of the Convention deal with safety regulations, in particular, those to be observed by vessels engaged in the laying of submarine cables, and by other vessels, including fishing vessels, which are at the location of a cable-laying operation, and with compensation issues.

Enforcement of the Convention is not limited to the flag State or State of nationality of the perpetrator.[50] According to Article X, commanders of warships or other State ships specially commissioned for that purpose are entitled to require the master of a merchant vessel suspected of having broken a cable to provide documentation regarding the vessel's nationality. The exhibition of such documents is to be endorsed immediately. The commander may then prepare a formal statement of the facts 'whatever may be the nationality of the vessel incriminated.' Those statements may be amended by declarations of the accused and the witnesses. Article X merely states that those statements 'may be considered, in the country where they are adduced, as evidence in accordance with the laws of that country', which, of course, implies that the statements will have to be transmitted to the authorities of the flag State. At first glance, the provision of Article X may indeed appear to be a 'curious arrangement.'[51] It must be borne in mind, however, that Article X is of the utmost importance for the right of States Parties to the Convention to stop and inspect (although in a most limited manner) foreign vessels

47 Article XV: 'It is understood that the stipulations of the present Convention do not in any way restrict the freedom of action of belligerents.' As regards the law of armed conflict applicable to submarine cable see *supra* note 6.

48 According to Article II (2), this 'provision does not apply to cases where those who break or injure a cable do so with the lawful object of saving their lives or their ship, after they have taken every necessary precaution to avoid so breaking or injuring the cable.' Other punishable offences are regulated in Articles V and VI.

49 It may be added that prior to the 1882 Paris Conference the Institut de Droit International 'rejected the contention that the destruction of cables should be assimilated to an act of piracy.' See Colombos (*supra* note 6), at p. 381.

50 Colombos, *ibid*.

51 S. Kaye, 'International Measures To Protect Oil Platforms, Pipelines, and Submarine Cables from Attack', 31 Tulane Maritime L.J. pp. 377-423, at p. 396 (2006-2007).

suspected of having committed an offence and to collect (and transmit) evidence.[52] This is a remarkable exception to the flag State principle. In the light of Article I, it could be argued that the right to stop and inspect foreign merchant vessels is limited to the warships and State ships of those States whose cables have, in fact, been damaged; the wording of Article X does not justify such a restrictive interpretation. Moreover, the object and purpose of the 1884 Convention is to effectively protect submarine telegraph cables in sea areas beyond national jurisdiction, and the States Parties have a common interest in ensuring the prosecution of those having wilfully or culpably damaged such cables. Hence, the warships and State ships of all Parties to the Convention are entitled to exercise the right under Article X.

In summary, the 1884 Convention has established a rather limited legal regime for the protection of submarine telegraph cables in sea areas beyond the outer limit of the territorial sea which, in those days, was limited to a breadth of three nautical miles (nm).[53] Although its scope of applicability is limited to submarine telegraphic cables and to acts committed by private actors, this does not mean that interference with a foreign submarine cable by State actors was considered lawful if it occurred during peacetime.[54] According to general international law, States may either claim a violation of their own rights or they may assert claims on behalf of injured parties incorporated or present within their jurisdiction.[55]

3.2 The 1958 Geneva Conventions

At the time of the adoption of the 1884 Convention, it was an undisputed right of all States to lay submarine cables. Since the breadth of the territorial sea was limited to three nm, there was no necessity of explicitly recognising that right in an international convention. With the recognition of continental shelf rights, however, those rights had to be reconciled with the right to lay submarine cables that, by necessity, were placed on, or buried in, the seabed. In view of the common interest in preserving existing cables and the freedom to lay new submarine cables – a comparatively expensive and challenging undertaking – neither the ILC, in its draft *Articles concerning the Law of the Sea,*[56] nor the States represented at the Geneva Conference seriously challenged the right of all States to lay submarine cables and their protection under the law of the sea.

52 In 1959, the US relied upon Article X when the USS *R.O. Hale* boarded the Soviet trawler *Novorossiisk* that had allegedly involved in the damaging of four telegraphic and one voice transatlantic cables. See 40 US Dept. of State Bulletin 555 (1959).

53 See Colombos (*supra* note 6), at pp. 88 *et seq.*

54 For the lack of a legal protection of submarine cables during an international armed conflict see *supra* note 6.

55 Wrathall (*supra* note 11), at p. 239. Moreover, cable owners (and operators) may have recourse to admiralty remedies in national courts of the home country of the perpetrators. See Green / Burnett (*supra* note 11), at p. 563.

56 *Supra* note 44.

Accordingly, the 1958 *Geneva Convention on the Continental Shelf,*[57] in Article 4, provides that the rights of the coastal State to the continental shelf do not include the right to prohibit the laying of submarine cables. However, the coastal State is entitled to 'take reasonable measures for the exploration of the continental shelf and the exploitation of its natural resources.'[58] What measures qualify as 'reasonable' has not been defined. Since the same exception has been included into the 1982 LOSC, we will return to this issue later.

The right of laying submarine cables has also been recognised in the 1958 *Geneva Convention on the High Seas* (1958 High Seas Convention).[59] According to Article 2(4), the high seas freedoms include the right of all States to lay submarine cables. The freedoms of the high seas shall be exercised with 'reasonable regard to the interests of other States in their exercise of the freedom of the high seas.' The right is reemphasised in Article 26(1).[60] Article 26(2) provides: 'Subject to its right to take reasonable measures for the exploration of the continental shelf and the exploitation of its natural resources, the coastal State may not impede the laying or maintenance of such cables or pipelines.' The remaining provisions of Articles 26(3), 27, 28 and 29 are almost identical with the respective rules already agreed upon in 1884. There is, however, a significant difference, insofar as the 1958 High Seas Convention does not explicitly provide for the right of warships and other State ships to identify the nationality of a merchant vessel suspected of having broken a submarine cable and to investigate the facts. Seemingly, enforcement of the rules on the protection of submarine cables has, thus, been reserved to the exclusive (criminal) jurisdiction of the flag State or the State of nationality.[61] It could be argued, however, that the right under Article X of the 1884 Convention has survived by virtue of Article 30 of the 1958 High Seas Convention, which provides that the 'provisions of this Convention shall not affect conventions or other international agreements already in force, as between States Parties to them.' Hence, in particular, those States that are bound by the 1884 Convention would be entitled to continue to apply Article X because their membership in the 1958 High Seas Convention has not rendered the former Convention obsolete.

It is important to note that the concept of a protection zone for submarine cables (and pipelines) did not find the necessary consensus. The ILC considered submarine cables in the same context as pipelines.[62] With regard to the latter it had been proposed to allow States to establish a safety zone of 250 metres on either side 'in which ships are

57 *Geneva Convention on the Continental Shelf* of 29 April 1958, 499 UNTS 311.

58 Article 4 reads: 'Subject to its right to take reasonable measures, the coastal State may not impede the laying or maintenance of submarine cables or pipelines on the continental shelf.'

59 *Supra* note 38. For a summary of the provisions see also Colombos (*supra* note 6), at p. 382.

60 'All States shall be entitled to lay submarine cables and pipelines on the bed of the high seas.'

61 Kaye (*supra* note 51), at p. 418; Wrathall (*supra* note 11), at p. 241.

62 In the beginning of its deliberations, the ILC decided against an inclusion of pipelines. See also O'Connell (*supra* note 43), at p. 508.

not to anchor and trawlers are forbidden to fish.'[63] This proposal was rejected because acceptance of such a safety zone was considered as unnecessarily impeding the freedom of navigation.[64]

3.3 The 1982 United Nations Convention on the Law of the Sea

The provisions regarding submarine cables of the 1958 Geneva Conventions and some of the 1884 Convention have found their way into the 1982 LOSC.[65] By including rules on submarine cables laid in the territorial sea, in archipelagic waters and in the Exclusive Economic Zone (EEZ), the legal regime has become more detailed. However, there still are some unsettled issues and ambiguities regarding the relationship between the rights of coastal States on the one hand and States exercising their right to lay submarine cables on the other hand. Moreover, the generally accepted interpretation of some of its provisions seems to limit considerably the rights of States to exercise jurisdiction over the submarine cables they (or their nationals) have laid, thus leaving those cables partly unprotected against malicious interference by State and non-State actors.

3.3.1 Territorial Sea and Archipelagic Waters

The sovereignty of coastal States extends to the territorial sea whose breadth may not exceed 12 nautical miles.[66] The coastal State's right to exercise jurisdiction (prescribe and enforce) in its territorial sea includes the right to regulate the laying, maintenance, repair, and replacement of submarine cables.[67] Although that right is limited by the right of innocent passage[68] and, in case of an international strait, the right of transit passage,[69] the coastal State, according to Article 21(1)(c) LOSC, 'may adopt laws and regulations, in conformity with the provisions of this Convention and other rules of international law, relating to innocent passage through the territorial sea, in respect of', *inter alia*, 'the protection of cables and pipelines.' According to Article 21(4), 'foreign ships exercising the right of innocent passage through the territorial sea shall comply with all such laws and regulations.'

---

63 YBILC 12 (1956 II).

64 In his report, the Rapporteur, M. François, stated: 'The Rapporteur believes that such a prohibition would constitute a further encroachment on the freedom of navigation and fishing and that it is consequently unjustified. It would prove very difficult, in practice, to mark the limits of such a zone. In the Rapporteur's opinion, the provisions of Article 35 of the draft articles on the regime of the high seas are sufficient'; YBILC 12 (1956 II). Draft Article 35 referred to eventually became Article 27 of the 1958 *Geneva Convention on the High Seas*.

65 *Supra* note 1. See also the *Agreement relating to the Implementation of Part XI of the United Nations Convention on the Law of the Sea of 10 December 1982*, of 17 August 1994, UN Doc. A/RES/48/263, entry into force on July 28, 1994.

66 Articles 2 and 3 LOSC.

67 See also *Tallinn Manual* (*supra* note 6), at pp. 17 *et seq*.

68 Articles 17 to 20 LOSC.

69 Article 38 LOSC.

In case of an archipelagic State, sovereignty also extends to the archipelagic waters as defined by archipelagic baselines.[70] Subject to the rights of innocent passage[71] and archipelagic sea lanes passage,[72] an archipelagic State has the right to regulate the laying, maintenance, repair, and replacement of submarine cables in its archipelagic waters and, according to Article 21(1)(c) LOSC, in its territorial sea. However, according to Article 51(2) LOSC, an archipelagic State must respect existing cables 'laid by other States and passing through [their] waters without making a landfall.' It shall, moreover, 'permit the maintenance and replacement of such cables upon receiving due notice of their location and the intention to repair or replace them.'[73]

3.3.2 Sea Areas Not Subject to Sovereignty

3.3.2.1 Right to Lay Submarine Cables

According to the 1982 LOSC and customary international law, all States have the right to lay submarine cables in sea areas that are not subject to the sovereignty of coastal States. This right is an integral part of the customary freedom of the high seas,[74] which also applies in the EEZ.[75] Interestingly, the laying of submarine cables on the continental shelf of another State, according to Article 79(1) LOSC, is not considered as a high seas freedom but as a right of its own.[76] In all instances, the exercise of the right to lay submarine cables is not unlimited, but subject to the rights of the coastal State and of other States exercising the freedom of the high seas.[77]

There is general agreement that the right to lay submarine cables includes all preparatory measures that are necessary to identify the appropriate route, as well as the right to maintain and repair a submarine cable.[78] According to the position taken here, it includes the right to replace existing cables.

---

70 Article 49(1) LOSC.

71 Article 52 LOSC.

72 Article 53 LOSC.

73 See also Beckman (*supra* note 45), at p. 4.

74 Article 87(1)(c) LOSC: 'The high seas are open to all States, whether coastal or land-locked. Freedom of the high seas is exercised under the conditions laid down by this Convention and by other rules of international law. It comprises, *inter alia*, both for coastal and land-locked States: [...] (c) freedom to lay submarine cables and pipelines, subject to Part VI.' See also Article 112(1) LOSC: 'All States are entitled to lay submarine cables and pipelines on the bed of the high seas beyond the continental shelf.'

75 Article 58(1) LOSC: 'In the exclusive economic zone all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in Article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention.'

76 Article 79(1) LOSC: 'All States are entitled to lay submarine cables and pipelines on the continental shelf, in accordance with the provisions of this article.'

77 See *infra* 3.3.2.2.

78 Beckman (*supra* note 45), at p. 5.

Identifying an appropriate route before laying a submarine communications cable is essential in order to 'minimise conflicts with other uses of the seabed, to minimise risks to natural hazards and man-made hazards, and to minimise the risk to particularly sensitive sea areas.'[79] In particular, the area of the seabed where a cable is planned to be laid has to be scrupulously scrutinised by hydrographic vessels.[80] A hydrographic survey 'may include measurements of the depth of water, configuration and nature of the natural bottom, direction and force of currents, heights and times of tides and water stages, and hazards to navigation.'[81] It is the 'science of measuring and depicting those parameters necessary to describe the precise nature and configuration of the seabed and coastal strip, its geographical relationship to the land mass, and the characteristics and dynamics of the sea.'[82] In sea areas subject to the sovereignty of the coastal State – territorial sea (including international straits) and archipelagic waters – such hydrographic survey activities may only be carried out with prior authorisation of the coastal States. In sea areas not covered by coastal State sovereignty, a hydrographic survey is an internationally lawful use of the sea that is closely related to the right to lay submarine cables that may be limited by the coastal State only to the extent that the law of the sea so provides. It needs to be emphasised that hydrographic surveys must be distinguished from 'marine scientific research'. Unfortunately, these concepts are not defined. According to an authoritative interpretation, 'marine scientific research' means 'those activities undertaken in ocean space to expand scientific knowledge of the marine environment and its processes.'[83] While marine scientific research in the EEZ and on the continental shelf may be regulated by the coastal State and only be conducted with that State's consent, hydrographic surveys can only be (partially!) regulated, if conducted on the continental shelf.[84]

If the right to lay submarine cables includes the right to repair them, it is obvious that the States (or their nationals) having laid and/or operating them must have the right to monitor and regularly inspect them. Again, this means that hydrographic survey ships and – manned or unmanned – submarines may be used for these purposes.

It is quite surprising that the replacement of existing cables has remained widely unnoticed. The average life-span of modern cables is limited to 20 years.[85] Many cables

---

79 *Ibid*., at p. 8.

80 *Ibid*., at pp. 8 *et seq*.

81 US Navy / US Marine Corps / US Coast Guard, *The Commander's Handbook on the Law of Naval Operations* (NWP 1-14M), para. 2.6.2.2 (July 2007).

82 G. Walker (gen. ed.), *Definitions for the Law of the Sea*, at p. 227 (M. Nijhoff 2012).

83 *Ibid*., at p. 241. See also NWP 1-14M (*supra* note 81), para. 2.6.2.1: 'Marine scientific research includes activities undertaken in the ocean and coastal waters to expand general scientific knowledge of the marine environment for peaceful purposes, and includes: physical and chemical oceanography, marine biology, fisheries research, scientific ocean drilling and coring, geological/geophysical scientific surveying, as well as other activities with a scientific purpose.'

84 See *infra* note 88 *et seq*. and accompanying text.

85 Sechrist (*supra* note 5), at p. 60. See also Appendix C with a list of existing cables landing in the US.

are also based on outdated technology. It is, therefore, foreseeable that many of the existing cables will have to be replaced in the near future. Although replacement is expressly dealt with only in Article 51(2) LOSC that applies to archipelagic waters, it is submitted that all States have the right to replace existing cables that are outdated or have become inoperable. Since the 19th century, States have been aware of the limited lifespan of submarine communications cables. There is a shared understanding that they are critical to the economy and security of all States. Limiting the right to repairing them instead of replacing them would oblige States (and their nationals) to invest considerable financial means into an existing cable, even though the repair would not necessarily extend the cable's lifespan. Hence, the fact that replacement of existing submarine cables is not expressly regulated in other provisions of the 1982 LOSC does not mean that it is not part and parcel of the right to lay submarine cables.

3.3.2.2 Limitations on the Right to Lay Submarine Cables in Sea Areas Subject to Coastal State Sovereign Rights

The right to lay (maintain, repair and replace) submarine cables is not unlimited. First, it is subject to the general obligation to pay 'due regard for the interests of other States in the exercise of the freedom of the high seas.'[86] This obligation is specified in Article 79(5) LOSC with regard to 'cables already in position. In particular, possibilities of repairing existing cables […] shall not be prejudiced.' Although Article 79(5) LOSC is part of the continental shelf regime, it addresses an obligation that also applies in other sea areas.[87]

More specific limitations on the right to lay submarine cables apply, if they are laid on the continental shelf or in the EEZ of another State. Although the continental shelf and the EEZ will, in most cases, be located in the same ocean space, it should not be forgotten that some coastal States are entitled to an extended continental shelf, provided that the respective criteria are met.[88] Therefore the provisions applying to the EEZ and to the continental shelf are not identical. However, this difference does not distinctly affect the right to lay submarine cables.

In the EEZ, the laying of submarine cables is limited by Article 58(3) LOSC.[89] It is important to note that the coastal State may only regulate activities in its EEZ insofar as

86 Article 87(2) LOSC.

87 According to Article 112(2) LOSC, it also applies in high seas areas.

88 Article 76(4)-(9) LOSC. It is not entirely clear whether claims to an extended continental shelf can be based upon customary international law. In view of the obligation, under Article 76(8), to submit claims to an extended continental shelf to the Commission on the Limits of the Continental Shelf, it seems that only States Parties to the LOSC are entitled to it. See also ICJ, *Case concerning Territorial and Maritime Dispute between Nicaragua and Honduras in the Caribbean Sea* (Nicaragua v. Honduras), ICJ Rep. 659, at p. 759 (2007); ICJ*, Territorial and Maritime Dispute* (Nicaragua v. Colombia), Judgment of 19 November 2012, MN 126 *et seq.*

89 Article 58(3) LOSC reads: 'In exercising their rights and performing their duties under this Convention in the exclusive economic zone, States shall have due regard to the rights and duties of the coastal State and shall

the laws and regulations are 'in accordance with the provisions of this Convention and other rules of international law.' It has been rightly stated that 'a coastal State would be able to regulate on subject matters attaching to the EEZ that might be relevant for the […] cable.'[90] In other words, under the EEZ regime, any regulation by the coastal State impacting upon the right to lay submarine cables would be justified only if necessary for the exercise of the EEZ rights recognised in Article 56(1) LOSC, i.e., exploration and exploitation, conservation and management of the natural resources, economic exploitation of the zone, establishment of installations, marine scientific research, and protection and preservation of the marine environment. In most cases, the laying of a submarine cable will not affect the exercise of the aforementioned rights or the natural resources and the marine environment. Although it cannot be ruled out that electromagnetic signatures can be detected in the vicinity of a submarine communications cable, it would probably exceed the limits of a reasonable interpretation if the introduction of such energy were considered a 'pollution of the marine environment', as defined in Article 1(1)(4) LOSC.[91] Hence, rules adopted by the coastal State that are aimed at the prevention, reduction and control of pollution of the marine environment may not impede or otherwise affect the right to lay submarine communications cables in the EEZ, unless they apply to cable ships.

On the continental shelf, the rights to lay submarine cables is subject to Part VI of the 1982 LOSC, i.e., to the rights enjoyed by the coastal State on the continental shelf.[92] As regards the rights of the coastal State to regulate submarine cables laid (or to be laid) on its continental shelf, Article 79 LOSC is of particular importance.

Although this provision deals with both submarine cables and pipelines, it 'makes important distinctions between them.'[93] The most significant difference exists with regard to the requirement of coastal State consent to the course of a submarine cable. According to Article 79(3) LOSC, this requirement only applies to submarine pipelines.[94] Hence, the delineation of the course for the laying of submarine cables is not subject to the consent of the coastal State.[95] The practice of some States, by which the consent

comply with the laws and regulations adopted by the coastal State in accordance with the provisions of this Convention and other rules of international law in so far as they are not incompatible with this Part.'

90 Kaye (*supra* note 51), at p. 401.

91 See also Takei (*supra* note 24), at p. 5.

92 Articles 87(1)(c) LOSC. See also Article 112(2) LOSC, according to which, 'Article 79, paragraph 5, applies to such cables and pipelines.'

93 Beckman (*supra* note 45), at p. 6.

94 Article 79(3) LOSC reads: 'The delineation of the course for the laying of such pipelines on the continental shelf is subject to the consent of the coastal State.'

95 See also Beckman (*supra* note 45) at p. 7, who adds: 'When read together, articles 79(2) and 79(3) seem to provide that the coastal State can take reasonable measures relating to the exploration of its continental shelf and the exploitation of its natural resources which put restrictions on the laying of submarine cables, but such measures may not require that the delineation of the course of a submarine cable on its continental shelf be subject to the consent of the coastal State.'

requirement is equally imposed on cables and pipelines, has no basis in the existing law of the sea.[96] The second difference exists with regard to 'reasonable measures' taken by the coastal State for the prevention, reduction and control of pollution that, according to Article 79(2) LOSC, may only be applied to pipelines, not submarine cables.[97] Against allegations to the contrary,[98] the 'coastal State has no right to impose conditions on the laying and maintenance of submarine cables for the protection, reduction and control of pollution.'[99]

The other provisions of Article 79 LOSC equally apply to pipelines and cables. The principal rule is that, according to Paragraph 2, a coastal State 'may not impede the laying or maintenance of such cables or pipelines', unless the measures taken qualify as 'reasonable measures for the exploration of the continental shelf [and] the exploitation of its natural resources.' Of course, the concept of 'reasonableness', despite its long-standing tradition in Anglo-American jurisprudence, is rather vague, and it is difficult to determine *ex ante* and in an abstract manner which measures can be considered as reasonable. Still, the wording as well as the object and purpose of Article 79(2) LOSC, make it possible to draw some basic conclusions. First, a measure would be unreasonable, if it resulted in the impossibility of laying a submarine cable, or if the costs would increase disproportionally. It should not be forgotten that modern submarine cables are considerably costly, and that every extension in length of one kilometre could increase the costs by US $75,000.[100] Second, a measure of a discriminatory character would not qualify as reasonable. Third, the measure must be necessary for the exploration and exploitation of the natural resources. Hence, 'it would seem reasonable for a coastal State to impose restrictions on the laying of submarine cables in the richest fishing grounds or coral reef areas in its EEZ and to put restrictions on the laying of cables in areas designated for off-shore exploration for oil and gas.'[101] Measures unrelated to the coastal State's sovereign rights of exploring and exploiting the natural resources and of other activities for the economic exploitation and exploration of the EEZ would fall outside the scope of Article 79(2) LOSC.

Finally, the coastal State may, according to Article 79(4) LOSC, 'establish conditions for cables or pipelines entering its territory or territorial sea, or its jurisdiction over cables and pipelines constructed or used in connection with the exploration of its

96 See the references to the practice of China, India, Malaysia, and Pakistan by Takei (*supra* note 24), at p. 7.

97 Article 79(2) LOSC reads: 'Subject to its right to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources and the prevention, reduction and control of pollution from pipelines, the coastal State may not impede the laying or maintenance of such cables or pipelines.'

98 See Takei (*supra* note 24), at p. 7, who holds that 'coastal states would be able to impose the consent requirement on the delineation of submarine cables in areas where the vulnerability of marine ecosystems indicates the necessity of such a requirement.'

99 Beckman (*supra* note 45), at p. 6.

100 See Sechrist (*supra* note 5), at p. 104.

101 Beckman (*supra* note 45), at p. 9.

continental shelf or exploitation of its resources or the operations of artificial islands, installations and structures under its jurisdiction.' This does not mean that, thus, the coastal State would be entitled to impose conditions on the laying of submarine cables on its continental shelf or in its EEZ that go beyond those provided for by the other provisions of Article 79 LOSC. Rather, the wording of Paragraph 4 – 'nothing in this Part affects the right' – suggests that the provision is to preserve the coastal State's right to impose additional restrictions on submarine cables laid in its territorial sea or in its territory. 'The fact that a submarine cable lands in a State's territory or passes through its territorial sea is not a justification for the coastal State imposing measures on the laying of a cable on its continental shelf which would not otherwise be 'reasonable measures' under Article 79(2) LOSC.'[102] Similarly, the remaining part of Paragraph 4 is to preserve the coastal State's jurisdiction over submarine cables that are constructed or used in connection with the exploration and exploitation of the natural resources of the continental shelf or EEZ.

3.3.3 High Seas and Obligation to Enact Domestic Legislation

Further provisions of the 1982 LOSC deal with the laying of submarine cables in high seas areas, and with the obligation of States Parties to enact national legislation on the protection of submarine cables against breaking or injury and on compensation.

3.3.3.1 Submarine Cables in High Seas Areas

The right to lay submarine cables in the high seas has been recognised in Article 87(1)(c) LOSC and has been reinforced in Article 112(1) LOSC, which explicitly grants all States the right to lay submarine cables (and pipelines) 'on the bed of the high seas beyond the continental shelf.' Again, this right is not unlimited but must be exercised with 'due regard for the interests of other States […] and for the rights […] with respect to activities in the Area.'[103] In particular, 'States shall have due regard to cables […] already in position' and may not prejudice the repair of existing cables.[104]

3.3.3.2 Obligation to Enact Domestic Legislation

Articles 113 to 115 LOSC are almost identical with Articles I, IV, and VII of the 1884 Convention.[105] According to Article 58(2) LOSC, these provisions are also applicable in the EEZ. It may be added that concerns regarding whether these provisions apply at all

102 Beckman (*supra* note 45), at p. 7.

103 Article 87(2) LOSC.

104 Article 79(5) LOSC that, according to Article 112(2) LOSC, also applies to the 'bed of the high seas beyond the continental shelf.'

105 *Supra* 3.1.

to fibre-optic cables[106] are unfounded because there is general agreement that neither the LOSC nor customary international law differentiate between submarine cables because of their design and composition.[107]

Article 113 LOSC obligates States to 'adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications.' The obligation to enact domestic criminal legislation also applies to 'conduct calculated or likely to result in such breaking or injury' but not to 'any break or injury caused by persons who acted merely with the legitimate object of saving their lives or their ships, after having taken all necessary precautions to avoid such break or injury.' According to the wording, the breaking or injury of a submarine cable that is not 'liable to interrupt or obstruct […] communications' need not be made a punishable offence under domestic law.

Article 114 LOSC obligates States to enact national legislation 'necessary to provide that, if persons subject to its jurisdiction who are the owners of a submarine cable or pipeline beneath the high seas, in laying or repairing that cable or pipeline, cause a break in or injury to another cable or pipeline, they shall bear the cost of the repairs.' According to Article 115 LOSC, the same obligation applies in order to 'ensure that the owners of ships who can prove that they have sacrificed an anchor, a net or any other fishing gear, in order to avoid injuring a submarine cable or pipeline, shall be indemnified by the owner of the cable or pipeline, provided that the owner of the ship has taken all reasonable precautionary measures beforehand.'

In sum, the obligation to enact national legislation related to submarine cables is limited in two respects. First, it merely covers the breaking or injury of submarine cables. Second, it only applies to flag States of culpable vessels, and to the States of nationality of those having broken or injured a cable and of the owners of submarine cables. The question is whether these limitations may be understood as excluding the exercise of jurisdiction by other States, in particular, by States that wish to take active measures for the protection of the submarine cables they (or their nationals) have laid. A closely related question is whether Article X of the 1884 Convention can still be relied upon. We will return to these issues.[108]

3.3.4 Dispute Settlement

The compulsory dispute settlement procedures entailing binding decisions under Part V Section 2 LOSC apply to disputes between the States Parties on the interpretation

106 Takei (*supra* note 24), at p. 10.

107 See the references *supra* note 40 and accompanying text.

108 See *infra* 5.

or application of the provisions on submarine cables. The exceptions in Article 297 LOSC and the optional exceptions in Article 298 LOSC allow for no limitations on the applicability of Section 2. Rather, Article 297(1)(a) LOSC expressly provides that 'disputes concerning the interpretation or application of this Convention with regard to the exercise by a coastal State of its sovereign rights or jurisdiction provided for in this Convention shall be subject to the procedures provided for in section 2 […] when it is alleged that a coastal State has acted in contravention of the provisions of this Convention in regard to the freedoms and rights of […] the laying of submarine cables.'

3.4 Preliminary Conclusions

Despite their importance for the economic and security interests of all States, the legal status of submarine communications cables is far from clear. While international law recognises the right of all States to lay submarine cables, it seems to be almost silent on the question as to whether and to what extent such cables are subject to the jurisdiction of the States that own them or whose nationals have laid and operate them. In particular, it is doubtful whether they are entitled to take the measures necessary to protect them against malicious interference. The provisions of the 1884 Convention and of Articles 113 to 115 LOSC are limited to an obligation to enact certain national legislation in order to ensure that 'a flag State will pursue individuals who damage submarine cables […] under their jurisdiction.'[109] Article X of the 1884 Convention on the right of the warships and other State ships of all States Parties to identify the nationality of a ship allegedly having broken a submarine cable and to establish the facts has not found its way into the 1982 LOSC.

The interests of coastal States on the one hand, and of States exercising their right to lay submarine cables on the other hand, have been adequately balanced by preserving the freedom to lay cables and by limiting the rights of coastal States to regulate foreign cable activities in the EEZ and on the continental shelf. Still, the right to lay submarine cables has come under increasing pressure by the well-known phenomenon of 'creeping jurisdiction', by which coastal States extend their jurisdiction to submarine cables beyond what is permissible under the 1982 LOSC and the corresponding customary international law.[110]

4. Is There Insufficient Legal Protection for Submarine Cables?

Since international law does not expressly provide measures for the protection of submarine cables beyond those provided by the 1982 LOSC, it seems that the current legal regime has gaps and loopholes, and that it no longer adequately protects submarine

109 Kaye (*supra* note 51), at p. 418.

110 For the establishment of cable protection zones by Australia and New Zealand see *infra* 4.2.1. See also Malaysia's *Continental Shelf Act* 1996, Act No. 57 of 28 July 1966, as amended by Act No. 83 of 1972.

cables. However, according to the position taken here, the alleged deficiencies of the existing legal regime are less grave than some believe. Moreover, it is to be expected that States will understand that they will have to exert increased efforts for the protection of submarine cables, nationally and internationally, if they wish to continue to benefit from this most important means of international communications. Hence, many of the proposals aimed at applying other legal regimes, or at amending the existing rules, are either premature or unnecessary.

4.1 (Alleged) Deficiencies of the Existing Legal Regime

It has been rightly stated that 'the legislative history of the Geneva Conventions […] and of the Draft Caracas Convention [i.e., the 1982 LOSC] has made the situation ambiguous. Both contexts contain references to the matter, which have developed somewhat independently of each other, and between which there is some awkward cross-reference.'[111] Indeed, the provisions on submarine cables do not seem to provide a coherent and adequate legal regime ensuring an effective protection of submarine cables.

The provisions of Articles 113 to 115 LOSC have been characterised as 'clearly inadequate.'[112] However, not all arguments on which this verdict is based are necessarily convincing. The fact that the States Parties to the 1982 LOSC have been more than hesitant in adopting domestic legislation to enforce Article 113 LOSC can hardly be considered a deficiency of the existing legal regime.[113] The obligation under Article 113 LOSC is clear. States Parties not complying with it simply violate international law. Another less convincing argument is that Article 113 LOSC does not deal with intentional theft.[114] While it is true that some States may lack criminal jurisdiction over the intentional theft of submarine cables in sea areas beyond the outer limit of the territorial sea, this, again, does not prove that Article 113 LOSC is inadequate. More importantly, however, Article 113 LOSC does apply to intentional theft. As the incidents of cable theft that occurred in the past[115] have shown, a submarine communications cable can never be removed from the sea bed in its entirety. In all these instances the cables were cut at two locations and the respective part of the cable was removed. Hence, cable theft by necessity implies a breaking or injury as provided for in Article 113 LOSC.

Some authors also criticise the lack of universal jurisdiction and, in particular, the fact that 'neither the LOSC nor any other international instrument were drafted with

111 O'Connell (*supra* note 43), at p. 508.

112 Beckman (*supra* note 45), at pp. 13 *et seq*.

113 *Ibid*. See also Wrathall (*supra* note 11), at pp. 244 *et seq*.; Takei (*supra* note 24), at p. 10.

114 Beckman (*supra* note 45), at p. 15.

115 See the reference *supra* 2.2.

the possibility of an attack on […] cables in mind, let alone an underwater attack.'[116] Indeed, Article 113 LOSC creates neither a right nor an obligation to exercise universal jurisdiction. It is, however, far from clear whether there is indeed a need for universal jurisdiction in order to enhance the legal protection of submarine cables against malicious interference. Probably, the calls for an introduction of universal jurisdiction into the legal regime regarding submarine cables are due to an interpretation of Articles 113 to 115 LOSC and customary international law which is too narrow. It will be shown that these provisions do not result in excluding the exercise of jurisdiction by States other than the flag State or State of nationality.[117] If at all, the criticism of Articles 113 to 115 LOSC is justified only insofar as the wording may not be as clear as it ought to be.

Finally, there is a point of criticism that is well-founded. Beckman rightly holds that:

> One reason why the legal regime governing submarine cables has been neglected is that there is no agency in the UN system that is responsible for submarine cables. Submarine cables are arguably of interest to the UN Division on Ocean Affairs and Law of the Sea (UNDOALOS), to the International Telecommunications [sic] Union (ITU), to the International Maritime Organization (IMO) and to the Fisheries Division of the Food and Agricultural [sic] Organization (FAO). However, none of these agencies has assumed the responsibility to review and update the legal regime governing submarine cables.[118]

Moreover, the International Cable Protection Committee (ICPC),[119] an association established by the cable industry in which States are not represented, 'has no observer status with any of the UN agencies which have an interest in submarine cables.'[120] It may be premature to demand a revision and update of the existing legal regime on submarine cables, but it would certainly contribute to legal clarity and to an enhancement of submarine cable protection if an international organisation took up the issue of protecting them, and if it invited the cable industry to play an active role.

4.2 Proposals for Improving the Legal Protection of Submarine Communications Cables

In the recent past, some proposals aimed at the improvement of the (allegedly) deficient international legal regime regarding submarine communications cables have been submitted. Some of these are interesting but, although of a potentially norm-creating character, they sometimes lack a basis in the *lex lata*.

---

116 Wrathall (*supra* note 11), at p. 248. See also Beckman (*supra* note 45), at p. 14; Kaye (*supra* note 51), at pp. 419 *et seq*.; Takei (*supra* note 24), at pp. 16 *et seq*.

117 See *infra* 5.

118 Beckman (*supra* note 45), at p. 16.

119 For more details, see the ICPC website at: http://www.iscpc.org.

120 *Ibid*.

4.2.1 Cable Protection Zones

Some authors[121] advocate the creation of cable protection zones or corridors that would not restrict navigation, but would prevent certain activities, such as anchoring, bottom trawling, sand mining, which pose some of the biggest threats to the integrity of submarine communications cables.[122] According to Stuart Kaye, the 'width of such a zone could be relatively modest, and probably be no more than 500 metres at best.'[123] Although a proposal to that effect was rejected by the ILC (and by the 1958 Geneva Conference)[124] and, although the concept was not taken up during the Third United Nations Conference on the Law of the Sea, these authors take the position that, in view of the minor interference with the exercise of the freedom of the high seas, such protection zones would have a basis in the international law of the sea as it currently stands.

The most comprehensive and elaborate justification of submarine cable protection zones has been provided by Kaye in a submission on the proposed protection zones off Sydney, Australia,[125] in which he holds that the protection of submarine cables by protective zones is in accordance with the law of the sea, if limited to certain protective measures (linked to the jurisdiction enjoyed by the coastal State within its EEZ or continental shelf). Kaye explains his findings as follows: whereas a coastal State would be entitled to establish a protective zone for submarine cables within its territorial sea according to Article 21(1)(c) LOSC,

> [o]utside of the territorial sea, there is no explicit legal basis to assert jurisdiction over a submarine cable by a coastal State. However, [... a] protection zone for a submarine cable outside the territorial sea could be validly asserted by Australia, providing the basis of jurisdiction was tied to a basis of jurisdiction that could be claimed under the regime of the EEZ or continental shelf. That is to say, protection over a cable could be achieved by restricting activities which could be validly regulated in the EEZ or continental shelf. […] The jurisdiction to deal with environmental protection in the EEZ would also provide a basis for jurisdiction for some of the activities sought to be prohibited. […] Similarly, Australia has jurisdiction over exploration and exploitation activities on the seabed in the EEZ and continental shelf. As such restrictions that prevent drilling in the vicinity of a submarine cable would also be valid at international law, not on the basis of the protection of a cable, but rather on the right of the coastal State to regulate drilling on the seabed on its continental shelf.

121 Kaye (*supra* note 51), at p. 422; Wrathall (*supra* note 11), at pp. 254 *et seq*.; Takei (*supra* note 24), at pp. 10 *et seq*.

122 See the references *supra* 2.2.

123 Kaye (*supra* note 51), at p. 422.

124 *Supra* notes 63 and 64.

125 S. Kaye, *Submission: Proposed Protection Zones Off Sydney*, October 26, 2006, available at: http://www.acma.gov.au/webwr/_assets/main/lib100668/professor%20kaye%20(uni%20of%20wollongong).pdf (last visited on 19 August 2013).

It is with no surprise that Australia[126] and New Zealand[127] were among the first to create cable corridors/protection zones that, within the territorial sea and EEZ, shield cables a mile on each side[128] from ship traffic and from other hazardous activities.[129]

It may well be that the cable protection zones established by Australia and New Zealand have proven to be 'successful from the perspective of an integrated management of competing activities in the oceans.'[130] It may well be that 'restricting transit or loitering within a prescribed distance from charted cables […] might ease the burden of attributing mal intent.'[131] However, cable protection zones and their location must be made public to international shipping, thus giving potential attackers almost perfectly exact information on their target.[132] Hence, such zones will only contribute to an enhancement of submarine cable protection against the usual threats posed by merchant and fishing vessels. They are not adequate for an effective protection against theft or other malicious interference, in particular by terrorists. Finally, their legality is far from clear, if cable protection zones are established in sea areas beyond the outer limit of the territorial sea. While Article 21(1)(c) LOSC provides a sufficient basis for cable protection zones within the territorial sea, there is no equivalent provision for either the EEZ or the continental shelf, and certainly not for the high seas. The freedom of navigation has already been curtailed by the progressive development of the law of the sea and by the growing tolerance *vis-à-vis* coastal State creeping jurisdiction. It is unlikely that the maritime powers will accept the concept of protection zones.[133] Hence, unless the law of the sea is consensually (!) modified to that effect, cable protection zones in sea areas beyond the territorial sea have no basis in the *lex lata*.[134]

126 Australia, *Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Act* (2005), No. 104, 2005.

127 New Zealand, *Submarine Cables and Pipeline Protection Act (1996)*, Public Act No. 22 of May 16, 1996.

128 'If the protection zone relates to more than one submarine cable, it consists of the area between the nominal location of the cables and the area within one nautical mile from the outside edge of the points on the surface of the sea above the nominal location of each of the two outermost cables', Takei (*supra* note 24), at p. 12, referring to Section 9 of the Australian Act.

129 Sechrist (*supra* note 5), at p. 51 and p. 80. For a detailed description of the protection zones established by Australia and New Zealand see Takei (*supra* note 24), at pp. 11 *et seq*.

130 Takei, *ibid*., at p. 14.

131 Wrathall (*supra* note 11), at p. 255, who adds: 'UUVs [unmanned undersea vehicles] entering the secure zone could be detected with passive sensors and possibly disabled. More consequentially, impeding mother ships from manoeuvring in close proximity to undersea infrastructure would force attackers to rely on the more dubious control and endurance of long-range, untethered UUVs to execute any underwater nefariousness.'

132 *Ibid*.

133 This view is shared by Kaye (*supra* note 51), at p. 422.

134 It may be added that, in his submission, Kaye (*supra* note 125) advises that, 'it might be prudent to restrict the zones to a distance of no more than 12 nautical miles from the coast. Beyond that distance, the restrictions ought to be restricted to fishing related activities, drilling and exploitation of the seabed and environmental matters such as scuttling or the use of a spoiling ground, to ensure that Australia complies with its international obligations.'

4.2.2 Universal (Criminal) Jurisdiction for Submarine Cable Depredations and Injuries?

In view of the importance of submarine communications cables for the global economy and international security it would, from a policy perspective, probably make sense to subject the breaking of such cables to the exercise of jurisdiction under the principle of universality. In the literature, there is some support for the exercise of universal jurisdiction over the breaking of submarine cables under the *lex lata*.[135] It is, however, not that convincing if these authors rely upon the (vague) domestic legislation of one State, on the (regional) 1928 *Convention on Private International Law*[136] (Article 308), and on the 1935 Harvard Research on International Law.[137] The wording of Article 113 LOSC and of its predecessors[138] is clear insofar as the exercise of criminal jurisdiction is concerned. Hence, there is no authorisation to exercise jurisdiction to punish the breaking or injury of a submarine cable beyond the outer limit of the territorial sea, unless the conditions indicated in Article 113 LOSC are met. Article 113 LOSC creates neither a right nor an obligation to exercise universal criminal jurisdiction.[139]

The 1988 *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* (SUA Convention), its Protocol and the 2005 amendments[140] were not drafted with a view to also protecting submarine communications cable against terrorist attacks. And, even if the wording of the 2005 amendments were to be interpreted in an excessively liberal manner, this would not provide States with a legal basis for boarding a foreign ship suspected of having broken or otherwise interfered with a submarine communications cable, because this 'would still require the flag State's authorisation, and obviously the flag State of the ship must be a party to the 2005 SUA Convention amendments.'[141]

---

135 Takei (*supra* note 24), at pp. 17 *et seq*. See also C. Ryngaert, *Jurisdiction in International Law*, at pp. 109 *et seq*. (Oxford University Press 2008).

136 *Convention on Private International Law*, Havana, 20 February 1928 (OAS, Law and Treaty Series, No. 34). The Convention, also known as the 'Bustamente Code', was adopted at the 6th International Conference of American States.

137 The Harvard Research on International Law, *inter alia*, produced the *Draft Convention on Jurisdiction with respect to Crime*, 29 AJIL, pp. 439 *et seq*. (1935 Suppl.).

138 During the 1958 Geneva Conference the Dutch delegate 'remarked that […] it was clearly not the intention of [Article 62 of the ILC Draft Articles] to enable any State to take legislative measures against nationals of another State causing injury to a submarine cable', United Nations Conference on the Law of the Sea, Geneva, 24 February – 27 April 1958, Official Records, Vol. IV, p. 88.

139 L.D.M. Nelson, 'Submarine Cables and Pipelines', in: *A Handbook on the Law of the Sea*, at p. 982 (ed. by R.-J Dupuy / D. Vignes, M. Nijhoff 1991); Kaye (*supra* note 51), at p. 418 *et seq*.

140 *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, Done at Rome, 10 March 1988 (entry into force: 1 March 1992); *Protocol of 1988 Relating to Fixed Platforms Located on the Continental Shelf*, Rome, 10 March 1988; *Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, London, 14 October 2005; *Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platform Located on the Continental Shelf*, London, 14 October 2005.

141 Kaye (*supra* note 51), at p. 420.

Finally, and against allegations to the contrary, the breaking of submarine communications cables does not constitute an act of piracy that would allow the exercise of universal criminal jurisdiction.[142] Of course, the proponents of that position are right if they emphasise that, according to Article 101(a)(ii) LOSC, illegal acts directed 'against a ship [..] or property in a place outside the jurisdiction of any State' also fall under the definition of piracy. Certainly, submarine communications cables qualify as 'property' and it would be possible to consider attacks against them as acts of piracy if those attacks took place in high seas areas. Moreover, any attack or other malicious interference by non-State actors would be committed 'for private ends.'[143] However, Article 101 LOSC must be interpreted in context with Article 113 LOSC. Such interpretation, by necessity, leads to the conclusion that the breaking of submarine communications cables has not been attributed to piracy and that the exercise of criminal jurisdiction, according to the prevailing consensus of States, is limited to the flag State or to the State of nationality of the perpetrator. Unless the definition of piracy is amended, the breaking of, or malicious interference with, submarine cables is not governed by the universality principle.[144]

4.2.3 Other Proposals

As seen, the majority of the proposals aimed at improving the protection of submarine communications cables do not necessarily have a basis in the law as it stands today. The ICPC recommends providing the exact coordinate route position lists of all cables to ship owners at their request in order to avoid inadvertent cuts.[145] 'However, this recommendation provides an easy way for seafarers to conduct malicious activity.'[146] In contrast, the ICPC recommendation to monitor the security of cable routes and corridors[147] seems to be an effective first step towards contributing to an enhancement of submarine cable security because, according to the position here, the right to lay submarine communications cables includes the right to monitor them in all sea areas beyond the outer limit of the territorial sea.[148] Of course, such monitoring is burdensome and expensive but, in view of the vital importance of submarine communications cables,

142 See, however, Green / Burnett (*supra* note 11), at pp. 573 *et seq.*; Beckman (*supra* note 45), at p. 15; Takei (*supra* note 24), at p. 18.

143 For a rejection of the widely-held view according to which 'for private ends' means the opposite of 'for political ends' see W. Heintschel von Heinegg, 'Repressing Piracy and Armed Robbery at Sea – Towards a New International Legal Regime?', 40 Israel Yearbook on Human Rights, pp. 219-241, at p. 223 (2010); D. Guilfoyle, 'Counter-Piracy Law Enforcement and Human Rights', 59 ICLQ, pp. 141-169 (2010).

144 See also Wrathall (*supra* note 11), at p. 256.

145 ICPC, *Actions for Effective Cable Protection (Post Installation)*, at pp. 4 *et seq.*, ICPC Recommendation No. 6, Issue 8A, of 27 September 2008.

146 Sechrist (*supra* note 5), at p. 46.

147 ICPC Recommendation (*supra* note 145), at pp. 8 *et seq.*, recommending the use of electronic means (radar, vessel monitoring systems – VMS, Automatic Identification Systems – AIS), as well as air, sea and terrestrial patrols.

148 *Supra* 3.3.2.1 and 3.3.3.1.

it is the best available means that does not infringe upon the freedom of navigation, which is far too important to be sacrificed for financial reasons or convenience.

5. Clarifying the Issue of Jurisdiction

It has been rightly stated that Article 113 LOSC 'does not make it clear which other states also have jurisdiction over the breaking or injury to submarine cables beyond the territorial sea.'[149] It is, however, questionable whether there is 'a presumption that a non-flag state is not recognised to exercise judicial jurisdiction against foreigners over the breaking of cables outside its own maritime zones.'[150]

Stuart Kaye seems to take the position that Article 113 LOSC is the final word on the exercise of jurisdiction in cases of malicious interference with submarine communications cables:

> If the severing of the cable took place outside the territorial sea of a coastal State, jurisdiction could only be based upon the nationality of the terrorists or the flag State of the ship, with only the latter possessing an immediate enforcement jurisdiction to deal with the offence. […] The coastal State probably lacks jurisdiction to intervene, even if it uses the affected cable, except possibly on the basis of self-defence. This is because the right to lay a cable is a high seas right, and matters affecting the cable do not fall within the EEZ jurisdiction the coastal State possesses, unless the action fails to show due regard for the rights of the coastal State in its EEZ. […] For a non-coastal State whose cable is interfered with, the case is just as difficult. Under the Law of the Sea Convention, such a State would have no basis whatsoever to arrest or impede an attack on its cable, unless it could categorise its response as self-defence. [151]

The latter view is shared by other authors.[152] While it is conceded that States bear international responsibility for acts attributable to them in accordance with the ILC's *Draft Articles on Responsibility of States for Internationally Wrongful Acts,*[153] the only remedies available in cases of interference with submarine cables are said to be either the right of self-defence (or an authorisation by the United Nations Security Council acting under Chapter VII of the *Charter of the United Nations*) or responsibility 'for shirking "jurisdictional control" over ships flying its flag in respect of "administrative, technical and social matters."'[154]

---

149 Takei (*supra* note 24), at p. 15.

150 *Ibid*., at p. 17, quoting Kaye (*supra* note 51), at pp. 418 *et seq*.

151 Kaye (*supra* note 51), at p. 419.

152 See also Beckman (*supra* note 45), at pp. 12 *et seq*.

153 International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts*, UN Doc. A/RES/56/83 of December 12, 2001.

154 Wrathall (*supra* note 11), at p. 243. See also Green / Burnett (*supra* note 11), at pp. 563 *et seq*.

As already mentioned, this position is based upon a too narrow interpretation of Article 113 LOSC. That provision merely deals with the obligation (!) to penalise the breaking or injury of submarine cables by the flag State or the State of nationality of the perpetrator. This does not imply the exclusion of an exercise of jurisdiction in other than criminal matters. States have accepted the obligation to enact domestic criminal legislation because they agree that submarine cables must be protected. Recognition of the obligation may not be considered a waiver of exercising jurisdiction in other matters or of taking the measures necessary to protect submarine cables against malicious interference. Hence, States having laid submarine communications cables, or whose nationals have laid and/or operate them, retain the right to exercise their jurisdiction in accordance with the well-established principles of international law, i.e., under the passive nationality and protective principle.[155] The fact that the jurisdiction of coastal States is limited by the rights enjoyed within the EEZ does not mean that coastal States that have laid, or are connected to a submarine communications cable, are no longer entitled to take protective measures. Finally, it would be a contradiction in evaluation if, on the one hand, the right to lay submarine cables is again and again emphasised and preserved but if, on the other hand, the States making use of that well-established right were legally barred from taking the necessary measures to protect them against threats that do not only exist in the minds of paranoid proponents of some kind of a conspiracy theory.

Hence, Article 113 LOSC merely excludes the exercise of criminal jurisdiction by States other than the flag State or State of nationality. Those States that have a valid interest in protecting 'their' submarine cables may not only exercise jurisdiction in other than criminal matters, but may also take all measures necessary for their protection. According to the position taken here, those measures include the identification of suspect vessels and the establishment of the relevant facts as provided for in Article X of the 1884 Convention.

However, in view of the uncertainties regarding the legal status of submarine communications cables and regarding the scope of jurisdiction interested States are entitled to exercise, a system of registration, 'giving the State of registration a limited ability to enforce laws to protect […] cables from interference'[156] would be the right choice. If the position taken here is shared, according to which Article 113 LOSC merely excludes the exercise of criminal jurisdiction, this solution is less 'radical' than it seems to be at first glance.

155 See also *Tallinn Manual* (*supra* note 6), at p. 23.

156 Kaye (*supra* note 51), at p. 423.

6. Concluding Remarks

The present international legal regime on submarine communications cables may not be perfect. It has been established with a view to protect these cables against the threats States were aware of in the 19th and in the second half of the 20th century. Still, this does not mean that States have thus waived their right to take all measures necessary to protect them against the threats that have materialised at the beginning of the 21st century. States whose nationals have laid and operate submarine communications cables have a legitimate right to protect them against malicious interference, be it by non-State actors, be it by State actors. It is, however, important to stress that submarine communications cables are legally protected only against depredation, breaking or other material damage. Unless they enjoy sovereign immunity, they are not expressly protected against other interference that does not result in interrupting or obstructing telecommunications. Despite the current commotion regarding the activities of the secret services of certain States, acts of espionage, like those allegedly conducted by the *USS Jimmy Carter*, are not prohibited under international law.

However, the protection of this critical submarine cyber infrastructure will improve only if States agree to entrust this task to an international agency or organisation, which will include the private cable industry. The existing structures are clearly inadequate. Moreover, States must establish an international public-private partnership in order to 'develop industry best practices, high-level operational exercises, reporting structures and comprehensive lists with single points of conduct.'[157] Finally, States should provide for financial and administrative incentives that will induce 'cable operators to build route diversity into the projects that face the necessity of replacing existing cables that will most probably run out of service within the forthcoming years.'[158]

157 Sechrist (*supra* note 5), at p. 7. See also Beckman (*supra* note 45), at p. 15.

158 Sechrist (*supra* note 5), at p. 60.

*Stefan A. Kaiser & Oliver Aretz**

Legal Protection of Civil & Military Aviation against Cyber Interference

1. Introduction and Scope

At present, cyber threats are only a minor concern in aviation, partly because of the development of aviation technologies in isolation from other technologies. This is changing, however, as the aerospace sector becomes increasingly dependent on information technologies. Air Traffic Management and aircraft are beginning to become vulnerable to cyber interference by State and non-State actors.

The scope of this chapter is the safety-critical functions of civil and military aviation. It does not cover computer reservation systems, electronic ticketing, passenger handling including check-in[1] and the use of non-certified electronic devices for safety-critical aspects of flight.[2] In the field of civil aviation this chapter analyses the existing regulatory, criminal and private law regimes in the context of cyber activities. In the field of military aviation it examines regulatory aspects and operational law in peacetime operations, but not the law of armed conflict and electronic warfare.

2. Technical Background

2.1 Technical Evolution of Aviation

For an analysis of aviation security with regard to cyber interference, the various elements of today's aviation system and its evolution must be understood. Aircraft, automated and unmanned aircraft systems, Communication, Navigation and Surveillance (CNS) and Air Traffic Management (ATM) are all interacting elements.

---

* Oliver Aretz contributed the sections on criminal and private law. This chapter is written by the authors in their personal capacity and shall not be attributed to NATO.

1 For example, the failure of airport check-in with subsequent flight delays in June 2011 due to sabotaged program code by airport subcontractor personnel for a dispute over a pay raise, see International Civil Aviation Organization (ICAO), *Working Paper to the Twelfth Air Navigation Conference* (19 to 30 November 2012), AN-Conf/12-WP/122, sec. 2.1. b).

2 For example, the use of non-certified so-called 'electronic flight bags' by flight crews for calculating aircraft performance parameters which may lead to flight incidents like tail strikes during take-off, see *Working Paper to the Twelfth Air Navigation Conference*, *ibid*, sec. 2.1. c).

2.1.1 Aircraft and Automated Aircraft Systems

Aircraft started as purely mechanical machines. Airfoils, fuselages, engines and mechanical flight controls like flaps, elevators and rudders were all derived from mechanics. As aircraft grew bigger, hydraulic and pneumatic actuators had to enhance human control inputs, but even early automation devices such as stabilizing gyroscopes and simple autopilots introduced before World War II remained in the realm of mechanics.

Following the rapid advance of computer technology for the United States (US) moon landing, aviation was the first industry to benefit from mobile computers for automated flight control and integration with radio navigation. The hard- and software of these onboard computers were developed independently from the mobile computers as they are known to the consumer market. They are more robust and hardware redundancy is ensured. Modern commercial aircraft are typically equipped with three independent computers for their Flight Management System.[3] When various onboard systems are computer controlled, the workload on the pilot is reduced.

Taking computerised flight control one step further, control surfaces and undercarriage are no longer activated mechanically, but rather by electrical systems linked to on-board computers; this is generally called 'fly-by-wire'. The increasing level of automation has led to a reduction in the flight crew from five or six about 60 years ago to typically two pilots in modern commercial airliners, despite the constant growth of aircraft size and complexity.

The next possible step will be for data links to connect the data streams to and from airborne computer systems. Aircraft systems and components, including command and control elements relevant for the safety and security of flight, can then be integrated into networks.

2.1.2 Unmanned Aerial Vehicles – Unmanned Aircraft Systems

The degree of automation reached a new level with 'Unmanned Aircraft Systems' (UAS).[4] Aircraft without pilots on board are operated by remote control and potentially, in the future, with partial or fully autonomous flight control systems that may substitute

3 A Flight Management System (FMS) is a specialised onboard computer system which provides navigational guidance based on a pre-programmed flight plan, input from navigational instruments and data bases. When linked to autopilot and auto-throttle, a FMS can control the flight path, attitude control and power setting in an integrated and dynamic manner.

4 The terms 'Unmanned Aircraft Systems' (UAS) and 'Remotely Piloted Aircraft Systems' (RPAS) emphasise the system approach and reach beyond the airborne unmanned vehicle itself. During the last few years, preferences for terminology have been changing and currently include for the unmanned vehicle 'Unmanned Aerial Vehicles' (UAV), 'drones' and 'pilotless aircraft'. 'Remotely Piloted Vehicles' (RPV), 'Remotely Operated Vehicles' (ROV) and 'Remotely Operated Aircraft' (ROA) are narrower terms which do not encompass fully autonomous vehicles.

for direct human involvement for long or short periods.[5] The International Civil Aviation Organization (ICAO) defines an unmanned aerial vehicle as

> [...] a pilotless aircraft […] in the sense of Article 8 of the Convention on International Civil Aviation[6], which is flown without a pilot-in-command on-board and is either remotely and fully controlled from another place (ground, another aircraft, space) or programmed and fully autonomous.[7]

The notion of UAS is based on the concept that an 'Unmanned Aerial Vehicle' (UAV) is not just an unmanned vehicle, but a more complex system consisting of several major elements.[8] UAVs were initially developed for military purposes, but the civilian market is seeing steep growth covering all kinds of aerial imaging for security, safety monitoring, research and environmental purposes. Several international governmental organisations are currently working on a civilian regulatory regime to ensure safety and possibly allow the operation of civilian UAVs in non-segregated airspace.[9]

2.1.3 Air Traffic Management

ATM[10] is presently undergoing technical changes and evolving from being airspace based to being so-called 'performance based' ATM.[11] This means that many air traffic control tasks will be automated. Airspace users will become more flexible in their choice of flight trajectories, which will be adjusted to user needs and aircraft performance. At the same time the airspace can be used more efficiently to accommodate higher traffic volume. All this will be made possible by information management with automated data

5 Despite autonomous operations being technically feasible, there are substantial legal and safety issues linked to the lack of human intervention and accountability during flight in a fully autonomous mode.

6 Article 8 of the *Convention on International Civil Aviation* (Chicago Convention), 1944 (Chicago), 15 U.N.T.S. 295 (ICAO Doc. 7300): 'No aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting State without special authorization by that State and in accordance with the terms of such authorization […].'

7 Endorsed by the 35th Session of the ICAO Assembly. See also ICAO, *Global Air Traffic Management Operational Concept* (ICAO Doc. 9854) and sec. 2.1 of the ICAO Circular 328 on Unmanned Aircraft Systems (UAS).

8 These elements include the UAV, the remote pilot station where the pilot-in-command handles the flight controls, the data links required for command and control, and the ground-based launch and recovery systems for smaller UAVs which do not take-off and land on runways.

9 ICAO Circular 138, *op. cit.* note 7; European Air Safety Agency (EASA), *Policy Statement – Airworthiness Certification Policy of Unmanned Aircraft Systems* (UAS), Doc. E.Y013-01, 25 August 2009; Kaiser, Stefan A., UAVs and Their Integration into Non-segregated Airspace, *Air and Space Law* 2011, 161.

10 The ICAO Procedures of Air Navigation Services (PANS-ATM, ICAO Doc. 4444), Chapter 1 define ATM as 'the dynamic, integrated management of air traffic and airspace including air traffic services, airspace management and air traffic flow management – safely, economically and efficiently – through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based functions.'

11 In Europe this technical evolution is foreseen by the Single European Sky Air Traffic Management Research (SESAR) program (www.sesarju.eu), and in the United States by the NextGen project (www.faa.gov/nextgen/).

exchange in real time with 'fail safe'[12] requirements. Thus, performance based ATM will rely heavily on information technologies and the use of enhanced communication networks.

2.1.4 Communication

Digital technologies have been introduced to aeronautical communication. Data communication supplements voice communication, and will replace much of it in the future. Coverage of aeronautical communication is becoming global, partly due to satellite communication, and encompasses ground-ground, air-ground, and air-air communication. The purpose of air-ground aeronautical communication systems has moved beyond traditional Air Traffic Service (ATS) Communication[13] and Aeronautical Operational Control (AOC).[14] Today there is an increasing amount of non-safety related communications such as Aeronautical Administrative Communication (AAC)[15] and Aeronautical Passenger Communication (APC).[16]

For ground-ground communications the Aeronautical Fixed Telecommunication Network (AFTN)[17] comprises fixed networks for voice and data between fixed stations of air navigation service providers, airports and government agencies. Originally designed for teletype communication, today's AFTN is based on internet protocol data formats.

2.1.5 Navigation

Navigation has advanced from terrestrial and astronomical means to radio navigation. Following medium wave, low precision, non-directional beacons (NDB), Very High Frequency Omni-Directional Range (VOR) ground radio stations, Distance Measuring Equipment (DME) and the Instrument Landing System (ILS)[18] became the backbone of aeronautical radio navigation in the 1960s. Since the 1990s the most evident changes to radio navigation are emerging Global Navigation Satellite Systems. After the Global Positioning System (GPS) of the USA other stand-alone systems with global coverage

---

12 A system is considered 'fail safe', when its design provides for (multiple) automatic back-up functions to avoid damage to life and property.

13 ATS Communication is safety related and covers communications executed by air traffic service units for air traffic control, flight information and alerting.

14 AOC is safety related and includes air-ground communication for flight operations, maintenance support, communications management, weather reports and position reporting to airline operations centers.

15 AAC is not safety relevant and consists of private correspondence of aircraft operators with their aircraft like scheduling, crew rotations and seat reservations.

16 APC comprises connections with onboard public correspondence facilities, like passenger telephone, messaging and internet, with public networks.

17 See also Annex 10 to the Chicago Convention, *op. cit.* note 6, Vol. III, Part I, Chapter 8.

18 For the technical specification of NDB, VOR, DME and ILS, see chapter 3 of Annex 10, Vol. 1, to the Chicago Convention, *op. cit.* note 6. ILS is a complex instrument precision approach system consisting of various ground based transmitting elements (localizer, glide slope and marker beacons, which require frequent and costly calibration) and the equivalent airborne receivers and indicators.

are following, such as the Russian GLONASS, the European Galileo, and the Chinese Beidou/Compass, as well as various regional satellite based augmentation systems and ground based augmentations of different nature and geographical scope.[19]

2.1.6 Surveillance

In the field of aeronautical surveillance there is a trend to supplement traditional primary and secondary radar with communication data links such as the Automatic Dependent Surveillance – Broadcast (ADS-B).[20] The Airborne Collision Avoidance System (ACAS),[21] which has become standard equipment in commercial aircraft and is mandatory in many air spaces, provides surveillance information to ACAS-equipped aircraft without the involvement of air traffic control.

2.2 Cyber Interference with Aviation

Cyber interference with aviation was not possible as long as aviation was undertaken exclusively by mechanical means. The introduction of CNS and computer systems, fly-by-wire controls, and the increasing trend of networking, increase the vulnerability of aviation to intentional and non-intentional cyber interference. It can affect an aircraft's flight control, ATM or remotely controlled payloads onboard.[22] Different methods of cyber interference can be distinguished, and include network hacking, jamming of radio data links, spoofing, or exploitation of design related vulnerabilities through the supply chain.

2.2.1 Hacking

Cyber interference is primarily associated with interference and hacking of networks which are connected to the internet. In aviation the Aeronautical Fixed Telecommunication Network (AFTN) is the network which resembles most closely the

---

19 For more details about existing and future satellite navigation systems see: United Nations Office for Outer Space Affairs, *Current and planned global and regional navigation satellite systems and satellite-based augmentation systems of the International Committee on Global Navigation Satellite Systems Providers' Forum*, New York, 2010, ST/SPACE/50.

20 ADS-B consists of two functions on an aircraft or vehicle: one 'that periodically broadcasts its state vector (position and velocity) and other information derived from on-board systems in a format suitable for ADS-B […] capable receivers', and another one 'that receives surveillance data from ADS-B […] data sources' (Annex 10 to the Chicago Convention, *op. cit.* note 6, Volume IV Chapter 1).

21 ACAS, also called TCAS (Traffic Alert and Collision Avoidance System), is 'an aircraft system based on secondary surveillance radar (SSR) transponder signals which operates independently of ground-based equipment to provide advice to the pilot on potential conflicting aircraft that are equipped with SSR transponders' (Annex 10 to the Chicago Convention, *supra* note 6, Volume IV Chapter 1). ACAS is mandatory for civil transport aircraft only. For technical details see Annex 10 Volume IV Chapter 4 and Attachment A of the Chicago Convention.

22 In military operations interference with payload control poses an intelligence threat. See for example Siobhan Gorman, Yochi Dreazen and August Cole, Insurgents hack U.S. drones - $26 Software is used to breach Key Weapons in Iraq: Iranian Backing Suspected, in *Wall Street Journal Europe* of 17 December 2009.

internet system architecture. Network segregation and coding are the standard tools to prevent unauthorised interference. Despite the evolution of onboard computer systems including fly-by-wire and Flight Management System (FMS), at the moment command and control functions of manned aircraft are not directly linked to ground-based stations. The situation is different in the case of Unmanned Aerial Systems, because they are controlled by a ground control station with a command and control data link. It seems only a matter of time until command and control functions of manned aircraft may also be connected to ground-based stations and possibly also to networks beyond.

2.2.2 Jamming and Spoofing

Currently, aircraft are more vulnerable to interference by external radio signals which can jam radio voice and data signals in CNS systems. Jamming is possible due to the low signal levels of CNS transmissions. With an increasing number of safety-related functions transmitted by radio, the vulnerability rises. Jamming leads to the loss of the usable signal and related functionalities, but this loss can be detected. More hazardous is the generation of bogus signals, so-called 'spoofing.' It is more difficult to detect an (intentional) wrongful signal that resembles, for example a navigation signal or the *false* surveillance signal of a non-existing aircraft.[23]

Jamming and spoofing may not only interfere through radio receivers, but also directly into the cable networks on an aircraft. The more information technologies and electrical systems are used on board, the higher is their vulnerability to electromagnetic induction. Even electronic devices with small electromagnetic footprints can intentionally or unintentionally interfere with electrical aircraft systems when used in the cabin of an aircraft.[24] Under special circumstances strong radio sources outside an aircraft can directly interfere with onboard systems, including the fly-by-wire flight controls.[25]

---

23 For example false broadcast messages of Automatic Dependent Surveillance (ADS-B) can be spoofed to create virtually images of (non-existent) aircraft. Inefficient use of airspace is the result, because air traffic controllers will establish separation for such virtual images, see ICAO, *Working Paper to the Twelfth Air Navigation Conference op. cit*. note 1, sec. 2.1.a.

24 For example the Transport Accident Investigation Commission New Zealand listed as findings in its *Aviation Occurrence Report 03-004* (paras. 3.10 and 3.11) that the controlled flight into terrain accident of Piper PA 31-350 Navajo Chieftain on 6 June 2003: 'The use of cellphones and computers permitted by the pilot on the flight had the potential to cause electronic interference to the aircraft's avionics, and was unsafe. […] The pilot's own cellphone was operating during the last 3 minutes of the flight, and could have interfered with his glide slope indication on the ILS approach.'

25 An early crash of an aircraft with fly-by-wire controls, a German Tornado fighter jet with two fatalities on 6 July 1984, was attributed to electromagnetic interference. The weekly *Der Spiegel*, no 33/1986 p. 70, referred to the German military accident investigation, which was said to have found that the crash must have been caused by electro-magnetic disturbance in the flight controls because of strong short wave emissions of the transmitter Free Europe.

2.2.3 Vulnerabilities through the Supply Chain

Cyber interference may also be introduced to automated aviation systems through the supply chain, when using commercial off-the-shelf (COTS)[26] hardware and software components. COTS components used in aviation or ATM designs increase the vulnerability to malicious software (malware). Cyber interference of this kind may either be triggered by outside intervention or be self-activated when certain conditions are met. The interference is made possible by mechanisms embedded in COTS hard- or software.

3. Civil Aviation and Cyber Interference

3.1 Regulatory Aspects

The ICAO has a lead role in establishing Standards and Recommended Practices (SARPS) for international civil aviation. Unless Member States notify differences, they have to implement standards in their national civil aviation regulations.[27] Through this mechanism ICAO has been successful in creating worldwide uniform technical standards for civil aviation. SARPS for security aspects of civil aviation are listed in ICAO Annex 17,[28] but they remain general. ICAO Annex 17 was amended in 2012 and since then includes one recommended practice which recognises cyber attacks as a threat to civil aviation and encourages Member States to develop countermeasures: 'Each Contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation.'[29]

Although more specific measures on security are contained in the Aviation Security Manual,[30] so far it 'does not include the problem of how future air traffic control systems are to be adequately secured'.[31] At the Twelfth Air Navigation Conference in November 2012 it was recommended that a ICAO cyber security task force should be established.[32]

---

26 Article 2, no. 19 of Commission Regulation (EC) No 482/2008 (30 May 2008) establishing a software safety assurance system to be implemented by air navigation service providers) defines 'COTS' as 'a commercial available application sold by vendors through public catalogue listings and not intended to be customised or enhanced'.

27 See Articles 37, 38 of the Chicago Convention, *op. cit.* note 6.

28 Annex 17 to the Chicago Convention, *op. cit.* note 6, Security – Safeguarding International Civil Aviation Against Acts of Unlawful Interference.

29 Annex 17 to the Chicago Convention, *op. cit.* note 6, sec. 4.9: Measures relating to cyber threats, Recommendation 4.9.1.

30 ICAO, Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (ICAO Doc. 8973/8) - access restricted.

31 ICAO, Working Paper to the Twelfth Air Navigation Conference, *op. cit.* note 1, sec. 1.6.

32 *Ibid.*

Today governmental cyber security policies and strategies, if they exist at all, tend to focus on internet-related threats and hardly touch upon aviation security.[33]

In the absence of more specific cyber security regulation, States should consider the following regulatory aspects for the protection of civil aviation *de lege ferenda*.

3.1.1 Make Cyber Security Part of Airworthiness Certification

States should mandate that protection against cyber interference becomes part of the certification of airworthiness. Cyber security standards need to be applied as airworthiness requirements to the entire civil aviation product, including its IT components.

It is not new to make aircraft security design elements part of airworthiness certification. Security driven design requirements include the least risk bomb location,[34] protection of the flight crew compartment, and interior design features to deter the concealment of weapons.[35] It is a plausible step to broaden such physical security measures to include designs to protect civil aircraft against cyber threats.

Certification of airworthiness is the responsibility of States. When States register civil aircraft for international navigation they shall provide a certificate of airworthiness. Such certificates are reciprocally recognised, provided that the requirements meet the standards established in ICAO Annex 8.[36] Since this is an elaborate exercise, the Federal Aviation Administration (FAA) of the US and the European Aviation Safety Agency (EASA) have *de facto* taken the lead and act as key institutions for the airworthiness certification of commercial civil aircraft.[37] Integrating cyber security requirements into

---

33 For example the only reference to aviation security in the US international strategy reads: 'Critical life-sustaining infrastructures that […] control air traffic […] all depend on networked information systems', see President of the United States, *International Strategy for Cyberspace, Prosperity, Security and Openness in a Networked World* (May 2011). The European Commission's strategy on cyber security does not mention aviation, see: European Commission High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7 February 2013, JOIN(2013) 1 final.

34 Standard 9.3.5 of Annex 8 to the Chicago Convention, *op. cit.* note 6, defines 'least risk bomb location' as a location 'where a bomb or other explosive device may be placed to minimize the effects on the aeroplane in the case of detonation'.

35 See Chapter 11 (Security – Airworthiness of Aircraft) of Annex 8 to the Chicago Convention, *op. cit.* note 6.

36 Article 31 of the Chicago Convention, *op. cit.* note 6. (Certificates of airworthiness): 'Every aircraft engaged in international navigation shall be provided with a certificate of airworthiness issued or rendered valid by the State in which it is registered.' Article 33 (Recognition of certificates and licenses) states: 'Certificates of airworthiness […] and licenses issued or rendered valid by the contracting State in which the aircraft is registered, shall be recognized as valid by the other contracting States, provided that the requirements under which such certificates or licenses were issued or rendered valid are equal to or above the minimum standards which may be established from time to time pursuant to this Convention.'

37 The standards of Annex 8 of the Chicago Convention, *op. cit.* note 6, remain too generic for the certification of aircraft and their components. It is left up to States to develop more detailed airworthiness codes and certification specifications (see also Foreword of Annex 8). National institutions typically fulfill their duties

the airworthiness certification complicates matters. Despite their lead role, the FAA and EASA have so far left the definition of electronic and IT standards to numerous specialised private institutions on which States rely for the safety and security of electronic components in civil aviation.[38] In the case of cyber security, States need to engage more directly. Even though the execution of security functions may be delegated to private bodies, the related regulatory prerogative and policy making need to be vested in States. They need to set minimum requirements for the managerial, operational and technical security measures.

3.1.2 Adopt an Anticipating Regulatory Approach for Cyber Security

Future aviation regulation of cyber security needs to be addressed in an anticipatory way. Safety regulations may already cover protection against electromagnetic interference and compatibility of electronic hardware, software and network protocols. Specifically for UAS, safety regulations need to include data links and ground based command and control stations. Nonetheless, for critical aircraft elements, regulation needs to reach beyond the safety aspects of electromagnetic interference and compatibility to encompass cyber security. Safety-critical aircraft elements are vulnerable against all kinds of *intentional* interference, including jamming, spoofing and hacking. For that reason it is not sufficient just to certify these elements for their safe operation, but also to ensure their security against intentional interference. Unlike the assurance of a sufficient level of probability to operate safely, future cyber threats must be anticipated.

A special challenge will be the higher speed of product development in the IT sector than in the safety-minded aviation industry. Electronic devices used for interference can progress more quickly than the certified aviation systems to be protected.

3.1.3 Avoid Commercial Off-The-Shelf Products in Safety Critical Functions

The use of commercial off-the-shelf (COTS) components should be avoided in aviation design. Traditionally aviation components were designed and manufactured solely for aviation purposes in order to achieve the highest quality standards and to meet aviation safety requirements. In recent aircraft designs there is a growing tendency to use COTS electronic hardware and software, including network protocols based on COTS

of certification for large civilian aircraft under Articles 31, 33 of the Chicago Convention by endorsing or re-validating the certifications of the FAA and EASA.

38 The ICAO, *Working Paper to the Twelfth Air Navigation*, *op. cit.* note 1, mentions: Eurocae/RTCA (aircraft/avionics manufacturing standards), A4A (Airlines for America) DSWG (Digital Security Working Group), IETF (Internet Engineering Task Force), CEN (European Committee for Standardization – *Comité Européen de Normalisation*), ETSI (European Telecommunications Standards Institute), AEEC (Airlines Electronic Engineering Committee).

products.[39] COTS hardware and software do not only complicate quality management through the supply chain, they also constitute gateways for cyber interference. Weaknesses of COTS products are already known to hackers. The commonality of COTS components in aircraft designs increases their vulnerability to known methods of interference, for example, by activating the hibernation mode of a known COTS component. Therefore, malware developed for non-aviation electronics can find its way into aircraft systems.

Functionalities for interconnection embedded into COTS components can also open 'backdoors' for interference to safety-critical aircraft systems: Ethernet, (wireless) LAN and blue tooth functionalities of ground command and control stations based on COTS components could connect a ground control station to the internet or a cell-phone. Therefore COTS components are not acceptable in networked flight control systems, such as flight control data links and ground stations of UAS.

3.1.4 Limit and Secure Network Interconnection for Aircraft Systems

A simple and yet efficient measure against cyber interference is to keep safety-critical fly-by-wire aircraft systems segregated from other existing networks. Traditionally airborne fly-by-wire systems and their data-buses[40] have been network 'islands'. Interconnectivity with other networks was not an issue. Future regulation must counteract the general trend of connecting isolated data islands when safety-critical aircraft systems are at stake and interference from third-party sources becomes feasible. Technical information, like the status of engines, is already transmitted en-route to operations and maintenance centres. A critical point will be reached, when data links allow direct access to flight controls and aircraft can be remotely controlled. Should such remote control capability be established for manned aircraft, the onboard pilot in command must have final control over all remote inputs, in such a way that he cannot be bypassed. Buffers or firewalls must be mandated to this end. Aeronautical Passenger Communication (APC) and on-board entertainment systems should be strictly separated from safety critical systems so that no common data-bus is used.

Radio interference with safety-critical aircraft systems is another area for regulatory measures. Despite the increasing practice of using Passenger Electronic Devices (PED) onboard aircraft, intentional or unintentional harmful interference, including wireless hacking of computerised flight controls, cannot be ruled out. Trends in recent years of relaxing in-flight restrictions on PEDs should not be taken for granted in light of

39 For example the Avionics Full Duplex Switched (X) Ethernet (AFDX) – also called ARINC-Standard 664 –, which is a derivative of the Ethernet, a signal protocol for (wired) Local Area Networks. AFDX is also used on the Boeing 787.

40 A data bus is a communication system used to transfer data between computer sub-systems or computers.

evolving consumer electronics.[41] The use of airborne fiber-optical data buses – 'fly by light' – can significantly reduce the vulnerability to radio interference.

3.1.5 Special Solutions for Interconnection in Air Traffic Management

Regulatory measures for cyber security of ATM need to be tailored differently. Interoperability is the hallmark of ATM.[42] With its Aeronautical Fixed Telecommunication Network (AFTN) as the backbone functionality of ATM, full physical network segregation does not appear possible, given the current state of the network hardware. The IT industry uses technical instruments and procedures such as encryption and firewalls to secure networks. Regulation needs to ensure that the technical means applied to safeguard the security of ATM reflects the state of the art. Regulation for ATM needs to link cyber security measures with the existing safety concepts that have always been the cornerstones of aviation regulation.[43] Operational safety and cyber security are the two sides of the same coin – including the case of ATM interconnection.

3.1.6 Maintain Redundancy and Diversity of Radio Navigation Systems

States should maintain a minimum level of radio navigation infrastructure that is independent of satellite navigation systems. The concepts of redundancy and system diversity need to be followed, whether information technologies are used in airborne or ground-based systems. Redundancy and system diversity are part of the aviation safety culture which successfully developed over many decades, and should not be undermined when introducing IT components.[44]

---

41 On 31 October 2013 the FAA announced that it had 'determined that airlines can safely expand passenger use of Portable Electronic Devices (PEDs) during all phases of flight' based on conclusions and recommendations of the PED Aviation Rulemaking Committee (ARC), U.S. Department of Transportation, Federal Aviation Administration, Press Release – *FAA to Allow Airlines to Expand Use of Personal Electronics*, <http://www.faa.gov/news/press_releases/news_story.cfm?newsId=15254>, see also *A Report from the Portable Electronic Device Aviation Rule Making Committee to the Federal Aviation Administration*, 30 September 2013, <http://www.faa.gov/about/initiatives/ped/media/ped_arc_final_report.pdf> This FAA decision is questionable in light of cyber threats. The ARC concluded that malicious use of PEDs was outside their scope and being addressed by other governmental agencies (2.2.2 of the report *ibid*). Although the FAA is the airworthiness authority of the aircraft, it passes the responsibility to demonstrate aircraft tolerance for expanded PED use to aircraft operators (recommendations 9, 10 of the report, *ibid*).

42 See for example the Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the Interoperability Regulation).

43 As examples of existing European Commission safety regulations for data links and software of air navigations providers, see: Commission Regulation (EC) No. 29/2009 of 16 January 2009 laying down requirements on data link services for the single European sky (Article 6.2. requires Member States to ensure that air navigation service providers implement an appropriate security policy for data exchanges, but does not specify such policy); and Commission Regulation (EC) No. 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005.

44 For more details about redundancy and systems diversity, see Stefan A. Kaiser, *Automation and Limits of Human Performance: Potential Factors in Aviation Accidents*, ZLW 2013, 207-208.

In the future, regulators and the civil aviation community should not rely on satellite navigation systems as the sole means of navigation and should resist the temptation to phase out traditional terrestrial navigation aids like VOR, DME and ILS. Despite the growing precision and robustness of satellite navigation systems,[45] their low signal levels make them vulnerable to cyber interference. [46]

Therefore States should maintain a minimum ground-based radio navigation infrastructure as a contingency against instances of cyber interference with satellite navigation. This is the role of States as expressed in Article 28 of the *Convention on International Civil Aviation* of 1944 (Chicago Convention):[47]

> [e]ach [ICAO] contracting State undertakes, so far as it may find practicable, to: […] [p]rovide, in its territory, […] radio services […] and other air navigation facilities to facilitate international air navigation, in accordance with the [ICAO] standards and practices recommended or established from time to time […].

For example, the US, even though it operates GPS and a national Wide Area Augmentation System, will maintain DME, VOR and ILS stations as independent navigation aids in the event of GPS outages due to radio frequency interference.[48]

3.2 Criminal Law

3.2.1 The Background

Since the 1960s civil aviation has, like no other means of public transport, continuously been the target of politically motivated crimes. From the first recorded hijacking on 21 February 1931, in Arequipa, Peru,[49] through the bombing of Pan Am flight 103 over Lockerbie, Scotland on 21 December 1988,[50] to the events of 11 September 2001 in New York City, USA, the attacks on civil aviation have been manifold. The international community has since tried to control the threat through the development of several conventions and protocols. While past attacks have been conducted with traditional kinetic force, the current pace and extent of new information technologies is notably

45 Because of an increasing number of satellites, ground-based augmentations and interoperability of open navigation signals. It is expected that in 2020 about 120 navigation satellites will broadcast interoperable non-encrypted signals.

46 See also Stefan A. Kaiser, Satellite Navigation Systems: The Impact of Interoperability, *Annals of Air and Space Law* XXXVII, 2012, 369.

47 *Op. cit.* note 6.

48 United States Department of Transportation, *Federal Radionavigation Plan 2012*, sec. 5.4.1. It also establishes a gradual reduction of the number of VOR stations by 2020, but not below a minimum operating network.

49 Jeffrey Price and Jeffrey Forrest, *Practical Aviation Security: Predicting and Preventing Future Threats*, Elsevier, 2009, p. 45.

50 United Kingdom, Air Accidents Investigation Branch (AAIB), Aircraft Accident Report No. 2/90 (EW/C1094); *Report on the accident to Boeing 747-121, N739PA at Lockerbie, Dumfriesshire, Scotland on 21 December 1988* (Doc. AAIB AAR 2/90 of 6 August 1990).

increasing the risk of malicious cyber activities.[51] With the introduction of COTS software and hardware into aircraft, the latest aircraft have a vulnerability to cyber attack that previous aircraft did not.[52] This poses the challenge of fitting the new threats into the current framework.

3.2.2 Hague Convention

In an attempt to combat skyjacking,[53] the *Convention for the Suppression of Unlawful Seizure of Aircraft* of 1970 (Hague Convention)[54] defines in Article 1: 'Any person who on board an aircraft in flight […] by force or threat thereof, or by any other form of intimidation […] commits an offence.'

A cornerstone of the application of the Hague Convention is that the offence has to be committed by 'a person on board an aircraft'. It is in the nature of the offense of skyjacking that the offender must be onboard the aircraft in order to take over its control. This excludes acts outside the aircraft, as for instance interception or kinetic attack. Given the realms of potential cyber interference, linking into the aircraft's internal systems and taking over control could be seen as an attack on board an aircraft, since the effect of the attack is taking place within the aircraft's internal systems. While at the time of the adoption of the Convention such scenarios seemed farfetched, proposals had been made within the ICAO Legal Committee and at the Hague Conference to extend 'unlawful seizure' to include acts committed by persons outside the aircraft.[55] The Conference, however, rejected this notion.[56] The Convention requires the seizure of aircraft or exercise of control to be from within.[57] Even if the effect of a cyber attack is felt inside the aircraft, in the sense of the Convention it must be considered as interference from the outside. Even more so, as the act is to be committed by a person on board and not by a person who would take control over the aircraft from outside its hull.[58] The Hague Convention of 1970 is therefore not the appropriate instrument to address cyber-related threats of seizing control of aircraft.

51 ICAO, Working Paper to the Twelfth Air Navigation Conference, *op. cit.* note 1, sec. 1.3.

52 United Kingdom, Centre for the Protection of National Infrastructure (CPNI), *Cyber Security in Civil Aviation* (August 2012), p. 5.

53 Yoram Dinstein, *Criminal Jurisdiction over Aircraft Hijacking*, 7 Isr.L. Rev. 195, 197 (1972).

54 *Convention for the Suppression of Unlawful Seizure of Aircraft*, 1970 (The Hague), 860 U.N.T.S. 105.

55 Rene Mankiewicz, The 1970 Hague Convention, 37 *J. Air L. & Com*. 195, 196 (1971).

56 *Ibid*.

57 Sami Shubber, Aircraft Hijacking under the Hague Convention 1970 – A New Regime? 22 *International and Comparative Law Quarterly*, pp. 687-726 (1973).

58 *Ibid*.

3.2.3 Montreal Convention

The international community quickly realised that the acts of violence perpetrated against civil aviation went beyond the simple act of hijacking, as aircraft were being sabotaged on the ground, bombs were being placed on board, and air navigation facilities were being interfered with, and so a new and broader international instrument was created with the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* of 1971 (Montreal Convention).[59, 60]

As such, Article 1 of the Montreal Convention significantly widens the scope of potential attacks or interferences with civil aviation:

> Any person commits an offence if he unlawfully and intentionally:
>
> a) performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft; or
>
> b) destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight; or
>
> c) places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight; or
>
> d) destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight; or
>
> e) communicates information which he knows to be false, thereby endangering the safety of aircraft in flight.

Evidently, Articles 1(b) through (e) no longer require an offender or his accomplices to be on board an aircraft to commit unlawful acts.[61]Article 1(b) is designed to deter and penalise acts of sabotage against the aircraft itself[62]. While such acts can be diverse, the definition leaves enough room to include acts of cyber attacks or interferences as described under section 2.2 of this chapter.

Article 1(d) of the Convention shifts the focus from the aircraft itself to the air navigation facilities. Currently, cyber interference with air navigation facilities seems to be the most viable intrusion, as long as aircraft are not fully automated. Following a report

---

59 *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, 1973 (Montreal), 974 U.N.T.S. 178.

60 Knut Hammarskjöld, Air piracy as an international crime: suggestions for international action, 32 *Int'l Rev. Crim. Pol'y* 14, 18 (1976).

61 Abraham Abramovsky, Multilateral Conventions for the Suppression of Unlawful Seizure and Interference with Aircraft Part II: The Montreal Convention, 14 *Colum. J. Transnat'l L.* 268, 282 (1975).

62 *Ibid*.

from the Korea JoongAng daily newspaper, the Seoul's Incheon Airport was target of such an attack on 15 September 2011.[63] While in this case the interference led only to delays in the departures of 18 airplanes, it is not hard to envisage a more severe effect in future attacks, especially considering that this particular airport will in the near future be able to handle up to 300 movements per hour. Any intrusion will lead to effects being immediately noticeable, be it due to inconvenience through delay or more dangerous situations, where for example airspace cannot be controlled safely any longer.

Article 1(e) attempts to deter those who intentionally communicate false information. While at the time of the drafting of the Convention, the technical focus was limited to radio communication, new integrated technologies allow for much further application of this provision, e.g. to use of digital means. Technical information and readings can also be falsified and jeopardise the safety of the aircraft.

The Convention does not apply to aircraft used in military, customs or police service. In accordance with Article 3 of the Convention, 'each contracting state undertakes to make the offences mentioned in Article 1 punishable by severe penalties.' According to a survey carried out by the ICAO, all States surveyed have provided in their criminal laws for the prosecution and punishment of offenders in a manner commensurate with the gravity of those crimes that seriously endanger the lives of passengers and crews.[64]

3.2.4 Beijing Convention and Protocol

Since the terrorist attacks on 11 September 2001, the international community has, with the *Convention on the Suppression of Unlawful Acts relating to International Civil Aviation* and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* of 2010 (Beijing Convention and Protocol),[65] tried to adopt new legal instruments to prevent repetition of this tragedy.[66] ICAO's review of existing law and other international dialogue sparked a negotiating process spanning almost nine years and leading to a diplomatic conference where these two new legal instruments emerged.[67] While intended to effectively replace the 1971 Montreal Convention and its 1988 Protocol,[68] to criminalise, for instance, the usage of aircraft as weapons and to

63 Lee Chul-Jae and Moon Gwang-Lip, Incheon Airport cyberattack traced to Pyongyang, *Korea JoongAng Daily* [online], 5 June 2012, <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2953940>.

64 Dionigi Fiorita, *Aviation Security: International Response*, 3 Alb. L.J. Sci. & Tech. 267, 279 (1993).

65 *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, 2010 (Beijing), ICAO Doc. 9960; *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*, 2010 (Beijing), ICAO Doc. 9959; both not yet in force.

66 Xiangqian Gong, The new development of International Law on Civil Aviation Security: The Beijing Convention and Beijing Protocol of 2010, 4 *J.E. Asia & Int'l L.* 232, 232 (2011).

67 Samuel Witten, Introductory note to the Convention on Suppression of Unlawful Acts relating to International Civil Aviation and the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, 50 *Int'l Legal Materials* 141, 141 (2011).

68 *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*,

facilitate prosecution and extradition of offenders,[69] the Beijing Agreements' are at this point not yet ratified.[70]

3.2.5 National Implementation

Therefore, at present, the 1971 Montreal Convention remains the only viable instrument to deter, prosecute and punish offenders who aim to endanger the safety of civil aviation by means of cyber interference. Following the Convention's Article 4, the international community has embedded these offences in national legislation.

For example, in Belgium Article 30 of the 1937 *Act amending the 16 November 1919 Act Regarding the Air Navigation Regulation* (*Wet van 27 juni 1937houdende herziening van de wet van 16 november 1919, betreffende de regeling der luchtvaart)* (as subsequently amended) states that: 'Anyone, who illegally and intentionally commits, or tries to commit an act, which might harm the airworthiness or safety of flight from a private or state aircraft will receive a punishment consisting of imprisonment from 10 to 20 years.' In the case of causing bodily harm to a person or the destruction of the aircraft, the punishment will be increased to 20 to 30 years imprisonment, while it will be further increased to life time sentence if the act results in the death of one or more persons.

Canada has implemented respective regulations not in a special aviation related act, but into section 77 of the *Criminal Code*:

> Everyone who, […] c) causes damage to an aircraft in service that renders the aircraft incapable of flight or that is likely to endanger the safety of aircraft in flight, […] e) causes damage to or interferes with the operation of any air navigation facility where the damage or interference is likely to endanger the safety of an aircraft in flight, […] g) endangers the safety of an aircraft in flight by communicating to any other person any information that the person knows to be false; is guilty of an indictable offence and liable for imprisonment for life.

As another example, section 315 of the German *Criminal Code* (*Strafgesetzbuch*) provides as such that:

> Whosoever interferes with the safety of traffic [...] by air by […] destroying, damaging or removing facilities or means of transport […] or undertakes a similar act of equal dangerousness and thereby endangers the life or limb of another person or property of significant value belonging to another shall be liable to imprisonment from six months to ten years.

1971 (Montreal), 1589 U.N.T.S. 474.

69 Xiangqian Gong, *op. cit*. note 66.

70 In accordance with Article 22, the Convention requires twenty-two instruments of ratification, acceptance, approval or accession. To date only 5 instruments of ratification and 3 instruments of accession are with the depositary. See ICAO, <http://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Conv_EN.pdf>.

The United Kingdom's (UK) *Aviation Security Act of 1982* implements the 1971 Montreal Convention into national law and makes in section 2 an offender liable to imprisonment for life.

3.2.6 Problem of Practical Application

Common to all national jurisdictions is the core problem of cyber related crimes: to identify offenders and attribute an attack in the absence of a claim of responsibility.[71] The issue lies with tracking down and getting access to the perpetrator. The options of actors are many. The attack may have been carried out by a State, a State sponsored group, an independent group, including terrorists and criminals, or a lone hacker.[72] Furthermore one not only has to protect oneself from external threats. Another, and potentially more severe, threat would be posed by the 'insider problem.'[73] There is potential for persons with intimate knowledge of the systems responsible for aircraft or ATM safety to abuse that knowledge. If targeted successfully, this could disrupt civil aviation operations on a broad scale.[74]

3.3 Private Law: Liability

Next to the question of how an offender can be punished, the issue arises how someone that sustained damages through the interference can seek redress. Here a difference needs to be made between persons on board an aircraft, those on the ground, and third parties.

3.3.1 Damage Sustained On-Board

Even though international air travel was still in its infancy, in 1929 an international regime for establishing unified rules for carriage by air and limiting liability was created and, in many respects, still applies today.[75] *The Convention for the Unification of Certain Rules Relating to International Carriage by Air* of 1929 (Warsaw Convention)[76] in its original form sought to protect the airline industry by providing a financial cap to claims, and to protect passengers by introducing a system of strict liability. It

71 Eurocontrol, *Manual for National ATM Security Oversight,* EUROCONTROL, Directorate Single Sky, 10/10/2012, V.1.0, p.14.

72 *Ibid*.

73 Hal Whiteman, Cyber Terrorism and Civil Aviation, in Sofaer, Abraham and Goodman, Seymour (eds.), *Transnational Dimension of Cyber Crime and Terrorism* (Hoover Press 2001), p. 73-89, at p. 78.

74 *Ibid*.

75 Tory Weigand, Accident, Exclusivity and Passenger Disturbances under the Warsaw Convention, 16 *Am.U.Int'l L.Rev.* 890, 899 (2001).

76 *Convention for the Unification of Certain Rules Relating to International Carriage by Air*, 1933 (Warsaw) 13, LON 137.

received several amendments intended to update, amongst other things, its financial compensation ceilings, although the ratification of these amendments is not uniform.[77]

Article 17 of the Warsaw Convention,[78] providing for personal injury claims, remained unchanged:

> The carrier is liable for damage sustained in the event of the death or wounding of a passenger or any other bodily injury suffered by a passenger, if the accident which caused the damage so sustained took place on board the aircraft or in the course of any of the operations of embarking or disembarking.

Additionally, according to Articles 18 and 19, the carrier also has to assume liability in the event of loss or delay of luggage or goods.

In attempt not only to update the Warsaw system, but also to capture all the various legal instruments which formed part of it, the international community created the *Convention for the Unification of Certain Rules for International Carriage by Air* of 1999 (Montreal Convention).[79] Whether this aim has been achieved or not remains debatable, and, depending on circumstances, the old system might still apply.[80] While not all nations have ratified the Convention,[81] it is safe to say that all major registration States for air carriers have adopted it.[82]

Whereas compensation levels have increased,[83] Article 17 of the Warsaw Convention has remained almost unchanged by the Montreal Convention and therefore the applicability of both systems in the case of a cyber inference may be assessed at once. While the death or wounding of a passenger may be determined with little room for interpretation, it is debatable what may constitute 'any other bodily injury.'

An aircraft incident may cause passengers shock or emotional distress. Unfortunately, in applying the conventions, courts have not been uniform.[84] The US Supreme Court has held that Article 17 does not allow for purely mental distress.[85] By contrast the Supreme

---

77 Detailed overview at <http://www.icao.int/secretariat/legal/Lists/Current%20lists%20of%20parties/AllItems.aspx>.

78 See *op. cit.* note 76.

79 *Convention for the Unification of Certain Rules for International Carriage by Air*, 2003 (Montreal), 2242 U.N.T.S. 309.

80 Bin Cheng, The Labyrinth of the Law of International Carriage by Air, 50 ZLW 155 (2001).

81 Currently ratified by 103 States and notably also the European Union under EC 889/2002. For current status see <http://www.icao.int/secretariat/legal/List%20of%20Parties/Mtl99_EN.pdf>.

82 *Op. cit.* note 75, 907.

83 Article 22 of the 1929 Warsaw Convention limited the passenger liability for the carrier to USD 8.300 (125.000 Francs), Montreal 1999 Article 21 sets it at USD 151.000 (100.000 Special Drawing Rights – SDR, see *infra* note 93).

84 Dafna Yoran, Recovery of Emotional Distress Damages under Article 17 of the Warsaw Convention: The American versus the Israeli Approach, 18 *Brook. J. Int'l L.* 811 (1992).

85 *Eastern Airlines vs Floyd*, 499 US 530, (S. Ct. 1991) 533.

Court of Israel concluded that such damage is recoverable.[86] Hence, while the outcome might depend on the State in which the claim is filed, the overwhelming majority of States will apply the Convention in the sense of a strict application of the term bodily injury (or *lésion corporelle* in its original, authoritative French text).[87] Therefore Article 17 requires in most cases an injury of not only emotional character.

As the Conventions do not provide a definition, national courts had to define the term 'accident' in their application and created non-uniform standards in the States party to the Conventions. The most notable definition in this regard was provided by the US Supreme Court, which held that an accident is an 'unexpected or unusual event or happening that is external to the passenger.'[88] It has also been established that an accident in the sense of the Convention may be caused not only by an air carrier's actions, but also through its inaction.[89] Courts have expanded the term 'accident' to include, among other things, injuries due to sexual and common assault, and to deaths due to Deep Vein Thrombosis.[90] Hence it is safe to say that, despite the ambiguity of the term 'accident', any cyber interferences leading to death, wounding or bodily injury of a passenger will constitute an accident in the sense of Article 17.

Article 20(1) of the Warsaw Convention provides for an exculpation of the carrier 'if he proves that he has taken all necessary measures to avoid the damage or if it was impossible for him to take such measures.' Hence, an unanticipated attack on an aircraft by means of cyber interference may excuse the carrier from its obligation for compensation. However, the courts have responded to hijackings, terrorist attacks and bombings on board international aircraft in the 1970s and 1980s by imposing liability for passenger injuries caused by these acts.[91] The key argument is that the carriers are in the best position to implement and enact safety measures,[92] and thus the airline industry should protect itself from malicious cyber activities.

Under Article 21 of the 1999 Montreal Convention, the rights of passengers were strengthened even more. A two-tier system has been introduced. Article 21(1) imposes a strict liability on the carrier of up to 100.000 SDR.[93] Above this amount, Article 21(2) allows an exculpation for the carrier. Common among all nations engaged in international

86 *Teichner v Air France Airlines* [1987] IsrSC 41(1) 589.

87 *Air France vs Saks*, 470 US 392, (S. Ct. 1985) 399.

88 *Ibid,* at 405.

89 *Olympic Airways v Husain* 540 US 644, (S. Ct. 2004) 12.

90 Domenica DiGacomo, The End of an Evolution: From Air France v. Saks to Olympic Airways v. Husain – The Term 'Accident' under Article 17 of the Warsaw Convention Has Come Full Circle, 16 *Pace Int'l L. Rev.* 409, 411 (2004).

91 Judith Karp, Mile High Assaults: Air Carrier Liability under the Warsaw Convention, 66 *J. Air L. & Com.* 1551, 1567 (2000-2001); see also *Haddad c. Air France* 1982 RFDA XXXIII Année 1979 327.

92 Karp, *op. cit.*, 1568.

93 SDR = Special Drawing Rights are supplementary foreign exchange reserve assets defined and maintained by the International Monetary Fund (IMF), see <http://www.imf.org/external/np/exr/facts/sdr.htm>.

air travel is a settled practice to apply these regimes. Under both systems, passengers on aircraft are generally entitled to compensation in case of injury through accidents. This is applied regardless of the cause or positive identification of the perpetrator, or the means of interference. Therefore the biggest challenge in cyberspace – the attribution of malicious cyber activities to the individual or entity responsible – is fortunately not an issue. While it would be too farfetched to say that the drafters of the Conventions already had foreseen possible cyber interference, the rules established as early as 1929 are solid enough to deal even with this new threat and – at least in this area – do not require amendment.

3.3.2 Third Party Damage

A first attempt to find an international regulatory framework was undertaken in 1933.[94] It received an update only 20 years later under the *Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface* of 1952 (Rome Convention).[95] The convention's aim was

> to ensure adequate compensation for persons who suffer damage caused on the surface by foreign aircraft, while limiting in a reasonable manner the extent of the liabilities incurred for such damage in order not to hinder the development of international civil air transport.[96]

Unlike the Warsaw Convention, it has not received universal ratification: at present 49 States are party to the treaty, including Spain, Russia, and the United Arab Emirates, but most of major international players in air carriage, including France, Germany, The Netherlands, the UK, and the US, have not ratified it.[97] Pursuant to Article I of the Rome Convention, '[…] any person shall be entitled to compensation if the damage was caused by an aircraft in flight or by any person or thing falling there from […].' Article 12 limits such compensation, for instance, in the case of loss of life to 500.000 Poincaré francs[98] (USD 50.000). Already at time of adoption, these limits were felt to be too low,[99] they seem even more outdated today, especially as one has to bear in mind that the innocent victim on the ground did not assume any risk, but may still lose his life or health and be

94 *Convention for the Unification of Certain Rules relating to Damage Caused by Foreign Aircraft to Third Parties on the Surface* (1933 Rome Convention) adopted in Rome on 29 May 1933.

95 *Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface*, 1952 (Rome), 310 U.N.T.S. 181.

96 Preamble, para. 1 of the 1952 Rome Convention, see *op. cit*.

97 For current status see <http://www.icao.int/secretariat/legal/List%20of%20Parties/Rome1952_EN.pdf>.

98 The Poincaré franc is defined as 65 1/5 of gold of millesimal fineness 900.

99 Gerd Rinck, Damage caused by Foreign Aircraft to Third Parties, 28 *J. Air L. & Com.* 405 1961-1962 (409).

denied full compensation.[100] Understandably, a need for improvement of the framework was apparent.[101]

The tragic events of the terrorist attack on the World Trade Center on 11 September 2001 invigorated the already ongoing modernisation process of the Rome Convention even further, and in 2009 two new international instruments were drafted and opened for signature and ratification, namely the *Convention on Compensation for Damage Caused by Aircraft to Third Parties* and the *Convention on Compensation for Damage to Third Parties Resulting from Acts of Unlawful Interference Involving Aircraft* (Montreal Conventions).[102] The Montreal Conventions are not yet in force, as they have to reach the required level of ratification. It remains doubtful that they ever will.

Therefore, in the majority of the cases, compensation for third-party damages will not be assessed under an international framework, but rather in accordance with the individual laws and policies of national jurisdictions, leading to some dissimilar results across the globe. To exemplify, a few national jurisdictions deserve a closer look.

Australia was originally party to the Rome Convention, but denounced the Convention in the year 2000, following the introduction of the national *Damage by Aircraft Act* in 1999. Owing to Section 10 of the act, a system of absolute liability was introduced, compelling the owner and operator of an aircraft jointly to compensate for any injury, damage, loss or destruction. The act does not provide a monetary ceiling on damages.

Following Article 33(1) of the German *Aviation Act* (*Luftverkehrsgesetz*) the owner of an aircraft is strictly liable to restore any damage to life, health or property of a third party. Article 37 of the act provides for certain caps, for example the maximum compensation for death or injury to a person is set at 600.000 EURO.

Prior to the use of aircraft, the common law already developed and applied a doctrine of absolute liability.[103] Such has found its way into the UK *Civil Aviation Act* of 1982. Section 76(2) of the act provides that

> […] where material loss or damage is caused to any person or property by […] an aircraft while in flight […] damages in respect of the loss or damage shall be recoverable without proof of negligence […] of the owner of the aircraft.

---

100 *Ibid*.

101 *The Protocol to Amend the Convention on Damage Caused by Aircraft to Third Parties on the Surface signed at Rome on 7 October 1952*, 1978 (Montreal), 2195 U.N.T.S. 372, aimed to raise those limits but only attracted 12 ratifications.

102 *Convention on Compensation for Damage Caused by Aircraft to Third Parties* (ICAO Doc. 9920) and the *Convention on Compensation for Damage to Third Parties Resulting from Acts of Unlawful Interference Involving Aircraft* (ICAO Doc. 9919), both done at Montreal on 2 May 2009, current status available at <http://www.icao.int/secretariat/legal/List%20of%20Parties/2009_UICC_EN.pdf> and <http://www.icao.int/secretariat/legal/List%20of%20Parties/2009_GRC_EN.pdf>.

103 *Rylands v. Fletcher* (1868) UKHL 1.

The act does not provide for any ceilings on the damage.

In 1922 the US adopted legislation to apply uniform rules among all of its States to impose an absolute and unlimited liability for ground damage upon aircraft users.[104] At the time it was argued that the person or owner of property on the ground is unable to avoid damage by aircraft, and hence the aviators must be held liable regardless of negligence.[105] This was based on the attitude at the time that flying was considered an ultra-hazardous activity, but, with the increase in safety, this view has shifted over the years, and this also shifted the US law from strict liability to a negligence-based system, based on individual State law, where the plaintiff now has to prove that damage was caused due to the negligence of the operator.[106] It is noteworthy that, after the events of 11 September 2001, the US Government introduced a federal act limiting the liability of air carriers and introducing a special victim's fund.[107]

The extent of an aircraft operator's liability for third-party damage depends first and foremost on the jurisdiction the claim may be filed under. If the subsequent damage has been caused by an interference with the aircraft through cyber means it does not alter the appreciation of the 1952 Rome Convention or the liability law of the individual States. The laws as they stand offer enough substance for a victim to file a claim and be awarded compensation. Most jurisdictions apply strict or absolute liability, but it is common that the aircraft operator will encounter difficulties when attempting to recover these damages from the perpetrator.

4. Military Aviation and Cyber Interference

The focus of this section is on cyber activities as a defensive means within the scope of the peacetime regime of cyber operations in military aviation. Technically, the methods of cyber defence within military aviation are similar to those in civil aviation. Yet the legal regime of military aviation, or more precisely the use of national airspace and the status of military aircraft, is fundamentally different.

4.1 The Status of Military Aircraft and National Airspace in Peacetime

The Chicago Convention[108] is not only the international foundation for a comprehensive safety regime for civil aviation, but it also safeguards sovereign control of Member States over their national airspace. Most prominently, Article 1 of the Chicago

104 United States, *Uniform Aviation Liability Act* (of 1922), Section 5.

105 William Schnader, Uniform Aviation Liability Act, 9 *J. Air L. & Com*. 664, 668 (1938).

106 Carel Stolker and David Levine, Compensation for Damage to Parties on the Ground as a Result of Aviation Accidents, *Air&Space Law*, vol. XXII, No. 2, 60, 61 (1997); see also *Boyd v White*, 128 Cal. App. 2d 641 and especially *Crosby v Cox Aviation Co. of Washington* 746 P.2d 1198 (Wash 1987).

107 *Air Transportation Safety and System Stabilization Act*, 22nd September 2001.

108 *Op. cit.* note 6.

Convention recognises the customary principle that every State has complete and exclusive sovereignty over the airspace above its territory and its territorial waters. Under Article 3 of this Convention military aircraft have the legal status of State aircraft, and as such are distinguished from civil aircraft. Along these lines, 'aircraft used in military, customs and police services shall be deemed to be state aircraft.'[109] This distinction has far-reaching implications. Firstly, the rules of the Convention do not apply to State aircraft.[110] Secondly, State aircraft require an 'authorization by special agreement' for the over-flight and the right to land in another contracting State.[111] Such an authorisation is typically given in a restricted manner by so-called 'diplomatic clearance'.[112] Consequently, military aircraft, like all State aircraft, are more restricted in the use of airspace than civil aircraft.

4.2 Regulatory Aspects

According to the language of Article 3 of the Chicago Convention, States may establish distinct regulatory regimes for their State aircraft. However, international cooperation and joint civil and military use of airspace have a converging effect in the fields of military airworthiness, interoperability and ATM. For the regulation of civil aviation, several aspects are addressed above as a matter of *lex ferenda*. For military aviation some additional points need to be added.

4.2.1 Airworthiness Certification

Similar to the envisaged certification regime for civil aircraft, it would also make sense to embrace protection against cyber threats in the airworthiness certification of military aircraft. This would not only be a mission-essential self-protection measure against electronic and network warfare, but also a matter of flight safety to be applied as an anticipatory approach.[113]

Unlike civil aviation, the certification of military aircraft, like all other State aircraft, is fragmented. Following the rule under Article 3(a) of the Chicago Convention, States apply either national military certification regimes or nothing close to civil aviation airworthiness. In many States, practices in regard to military aircraft certification are opaque. However, under Article 3(d) of the Chicago Convention, 'contracting States undertake, when issuing regulations for their state aircraft, that they will have due regard for the safety of navigation of civil aircraft.' In the European Union this 'due

109 *Ibid,* Article 3(b).

110 *Ibid,* Article 3(a).

111 *Ibid,* Article 3(c).

112 See for example United States Department of State, *Diplomatic Aircraft Clearance Procedures for Foreign State Aircraft to Operate in The United States National Airspace*, <http://www.state.gov/t/pm/iso/c56895.htm>.

113 See *supra* sections 3.1.1 and 3.1.2.

regard' principle was restated for the airworthiness of State aircraft.[114] As a further step, under the auspices of the European Defence Agency (EDA), European States wish to streamline the airworthiness of their military aircraft by a Military Airworthiness Authority (MAWA).[115]

In order to cover malicious cyber activities, rather than only safety-related electromagnetic interference and compatibility, military certification standards should be prescriptive and anticipatory, and not just be a 'safety case', collecting evidence to show that a system has proved to be safe in the past.[116]

4.2.2 Interconnection and Interoperability

Segregation of networks for safety and mission-critical functions remains one of the basic physical means against cyber interference. Traditionally, physical security measures have been key to military operations, regardless of whether electronic or paper-based military information is at stake. At first glance, interconnectivity of military flight control and mission control data does not appear to be a problem, but military information systems increasingly rely on civilian communications infrastructure. Physical segregation is not always possible any longer. Encryption and electronic fire-walls to non-classified networks thus also become defence lines for military information networks.

Another cyber vulnerability of flight and mission control stems from interoperability. Interoperability is a quintessential element for the cooperation of allied forces, but what started as the standardisation of ammunition has developed in far more sophisticated areas in the time of information technology. Interoperability of information systems for military aircraft, intelligence, surveillance and reconnaissance (ISR)[117] and

114 Regulation (EC) No. 216/2008 of the European Parliament and of the Council of 20 February 2008 concerning on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, Article 1, section 2.: 'This Regulation shall not apply when products, parts, appliances, personnel and organizations […] are engaged in military, customs, police, or similar services. The Member States shall undertake to ensure that such services have due regard as far as practicable to the objective of this Regulation.'

115 See for the approval by 21 States of the European Harmonized Military Airworthiness Basic Framework Concerning the Development, the Acceptance and the Implementation of European Military Airworthiness Requirements, <http://www.eda.europa.eu/info-hub/news/2013/06/19/european-defence-agency-reflects-on-the-need-for-greater-harmonisation-in-military-airworthiness>.

116 The United Kingdom's Royal Air Force applies the concept of safety cases also to the airworthiness of military aircraft. In accordance with the UK Defence Standard 00-56, Issue 4, Annex A, a 'Safety Case' is understood as 'a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.'

117 For definitions of ISR, see for example United States Air Force, *Air Force Basic Doctrine Document 1* (17 November 2003), pp. 54-56: '**Intelligence** is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Specifically, intelligence efforts will focus on: foreign military capabilities; political groups; political, social, and technological developments; or particular geographic regions. […] **Surveillance** is the function of systematically observing air, space, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. […] **Reconnaissance** complements surveillance by obtaining specific

weapons systems may become gateways for cyber interference. As a consequence, standardised interfaces for the interconnection of military flight control[118] and mission or payload control[119] need to be continuously improved to assure a sufficient level of security.

4.2.3 Air Traffic Management and Military Aircraft

The more military aircraft use non-segregated airspace with fully-fledged ATM services, the more ATM interconnection issues need to be addressed with regard to military aircraft. Although States may establish their own national regulatory regimes for airworthiness and operations of their State aircraft, there are limits when State aircraft are operated in the same airspace as civil aircraft, especially when operating under an 'authorization by special agreement' in foreign airspace. Compliance with the 'due regard' prerequisite of Article 3(d) of the Chicago Convention leads to increasing technical requirements when military aircraft use airspace with modern IT-based ATM. This was recognised by the Member States of the European Union when they established the Single European Sky concept. Although military aviation falls outside of the scope of the European Union, Member States agreed on a statement on military issues related to the Single European Sky.[120] Military aircraft participating in modern civilian CNS-ATM environments are subject to the same cyber vulnerabilities that affect civilian CNS-ATM.

4.2.4 Export Control

The enforcement of export control policies may in the future be supported by information technology components introduced during the design and fabrication process into military products like aircraft, missiles and precision-guided weapons. Proliferation of weapon systems is a major issue for arms-exporting States. National security interests and economic interests are not always in line, and they may change during the lifetime of a weapon system.

---

information about the activities and resources of an enemy or potential enemy through visual observation or other detection methods; or by securing data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.'

118 See for example the North Atlantic Treaty Organization (NATO) Standardization Agreement (STANAG) 4586 for Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability.

119 See for example NATO STANAG 5501: Digital Data Link 1 (Point to Point), STANAG 5516: Tactical Data Exchange - Link 16, STANAG 5511: Tactical Data Exchange - Link 11.

120 Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the Single European Sky (Framework Regulation) and Statement by the Member States on military issues related to the Single European Sky (attached to Regulation (EC) No 549/2004). These requirements are spelled out in more detail in Eurocontrol, Civil-military ATM Coordination Division, Communications-Navigation-Surveillance Unit, *White paper on performance-based certification of military airborne systems to meet civil ATM/CNS requirements* (Edition 1.0 of 6 March 2013).

It is technically conceivable for designers of military aircraft, missiles and 'intelligent' weapons to introduce dormant software into the system design to prevent such weapons being used against the territory or airspace of the originating State, or against its military assets, including military aircraft. The manufacturing State could retain the electronic 'master key' to take control of an adversary's weapon, including flight control of military aircraft or UAVs, when deemed necessary for national security. It is clear that customers of military products will reject this concept and spur the development of national defence products for that reason. Nonetheless software-embedded design features could be applied as a unilateral and covert solution for enforcement of national export control policies that is tailored to the affected territory, airspace or adversary.

4.3 Military Operational Law in Peacetime

Air policing and airborne ISR activities are standard military operations during peacetime and may increasingly encompass cyber operations, although not the full range of electronic and network warfare.[121]

4.3.1 Air Policing – Electronic Interception

Air policing is a standard military operation during peacetime, aiming at the enforcement of air power in a given airspace. It may be undertaken in national airspace, but also in international airspace for the protection of national airspace. Air policing includes the interception and, as a last resort, the shooting-down of non-compliant aircraft. Air policing may be directed against civil aircraft, often also referred to as 'renegade' aircraft, or State aircraft.[122]

Air policing is not undertaken under the law of armed conflict, but follows peacetime 'rules of engagement' established by governments for their national air forces. This legal framework differs from State to State. National details are classified. Nevertheless, it can safely be said that the purpose of these operational activities is to police and enforce the sovereign integrity and, if necessary, to act in (collective) self-defence. Military peacetime operations are also limited by international law applicable during peacetime.

121 The United States Air Force, *Air Force Basic Doctrine*, *op. cit.* note 117, pp. 46f, defines as follows: '**Electronic warfare operations** are those military actions involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy across the electromagnetic battlespace. […] **Network warfare operations** are the integrated planning and employment of military capabilities to achieve desired effects across the digital battlespace.'

122 See also the definition of air policing of the United States Department of Defense, *Dictionary of Military and Associated Terms* (2005): 'The use of interceptor aircraft, in peacetime, for the purpose of preserving the integrity of a specified airspace.'

4.3.1.1 Air Policing of Civil Aircraft

The reasons for air policing of civil aircraft can be navigational error, communication failure, or misuse of civil aviation,[123] such as when a civil aircraft transports weapons without authorisation by the overflown State or, as an extreme case, when a civil aircraft is intended to be used as a weapon. Following the principle of proportionality of State acts during peacetime,[124] military aircraft undertaking air policing must apply internationally recognised interception procedures[125] and may require an unauthorised civil aircraft to land at a designated airport or to give any suitable instructions to cease the violations.[126] Article 3 bis(a) of the Chicago Convention recognises a legal limitation:

> The contracting States recognize that every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of persons on board and the safety of aircraft must not be endangered. This provision shall not be interpreted as modifying in any way the rights and obligations of States set forth in the Charter of the United Nations.

The first sentence of Article 3bis(a) is the recognition of a customary law rule to protect lives on-board civil aircraft. Nonetheless, following the events of 11 September 2001, numerous States tend to interpret the right of self-defence – indirectly referred to in the second sentence – more broadly, which increases the tension between the two sentences of this provision.

In the context of peacetime military cyber operations, it is technically conceivable that in the future remote flight control could be exercised as an electronic means of interception. Electronic interceptions could be viewed as less risky than the physical interception practiced today, and reduce the possibility of the use of weapons against civil aircraft. Thus, electronic interception may be regarded as a less invasive tool-set. However, currently civil aircraft are not designed for electronic interception. There are no recognised procedures for access to remote flight control of civil aircraft in these circumstances.

Politically, electronic interception is highly questionable. It would strengthen the exercise of sovereign powers of States over their airspace to an unprecedented dimension – contrary to the international trend of increased cooperation in international air traffic

---

123 See also Article 4 of the Chicago Convention *op. cit.* note 6.

124 Proportionality of acts of State in peacetime must be understood here as a principle of justice and fairness to apply only such measures of enforcement that are suitable, necessary and proportionate to the severity of the violation. It is not to be confused with the proportionality principle of the law of armed conflict, which is to avoid excessive collateral damage.

125 For interception procedures, see Annex 2 to the Chicago Convention, *op. cit.* note 6, Rules of the Air, Attachment A., Interception of Civil Aircraft.

126 Article 3bis(b) of the Chicago Convention, *op. cit.* note 6. In accordance with Article 3bis(c) of the Chicago Convention, intercepted aircraft are obligated to comply; States are to implement relevant national rules including penalties for non-compliance.

and the use of congested airspace. At the same time the navigational authority of the pilot in command would be weakened.[127] It needs to be borne in mind that aircraft design features that allow for electronic interception could be misused, and it is doubtful that the benefits outweigh the risks of misuse by State and non-State actors.

Nevertheless, there is one application where electronic interception may have a future: air policing of civil UAVs. Remote flight control is a design feature of UAVs and no persons onboard are endangered. In the future, it could be possible that over-flown States require access to the remote flight control of civil UAVs as a requirement for the 'special authorization' under Article 8 of the Chicago Convention.

4.3.1.2 Air Policing of Military Aircraft

When military aircraft violate the airspace of another State it constitutes a violation of the sovereign integrity of that State in the meaning of Article 2(4) of the *Charter of the United Nations*.[128] Air policing within national airspace is a legal measure to deny, cease and prevent such violations, up to the use of force. The rules for the protection of civil aircraft recognised under Article 3bis of the Chicago Convention do not apply.

In the future, electronic interception of remote flight control could be considered by the State whose airspace is violated as a procedure to deny, cease and prevent such violations without the use of physical force. Although it is not acceptable for any air force to allow electronic interception or remote flight control by a foreign force, it cannot be ruled out that manufacturing States covertly embed, at the time of manufacturing, features into exported military products that allow electronic interception, at a later time, for export control or other reasons.[129]

4.3.2 Intelligence, Surveillance and Reconnaissance

ISR operations by military aircraft relate to information gathering by wireless means from airborne platforms and their subsequent communication.[130] ISR relevant frequency bands used by military aircraft are subject to line-of-sight radio wave propagation. The use of radio frequencies, whether for the active collection of information, eavesdropping,

127 Standard 2.3.1. of Annex 2 of the Chicago Convention, *op. cit.* note 6: 'The pilot-in-command of an aircraft shall, whether manipulating the controls or not, be responsible for the operation of the aircraft in accordance with the rules of the air, except that the pilot-in-command may depart from these rules in circumstances that render such departure absolutely necessary in the interests of safety.' Standard 2.4, *ibid*: 'The pilot-in-command of an aircraft shall have final authority as to the disposition of the aircraft while in command.'

128 Article 2(4) of the *Charter of the United Nations,* 1945, 1 U.N.T.S. XVI, reads: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.'

129 See section 4.2.4 *supra*.

130 This chapter does not address interference with or hacking of the internet for obtaining ISR.

spoofing or jamming have range limitations dependent on the position and altitude of the aircraft performing ISR.

Thus, during peacetime, States can limit the exercise of ISR by foreign aircraft in the airspace over their national territory by exercising their sovereign rights. Diplomatic clearances for flights of military aircraft in foreign airspace typically[131] prohibit ISR activities.[132] When exercising the right of transit passage through the airspace above international straits, (State) aircraft shall 'refrain from any activities other than those incident to their normal modes of continuous and expeditious transit unless rendered necessary by force majeure or by distress.'[133] This excludes acts 'aimed at interfering with any systems of communication or any other facilities or installations of the coastal State.'[134]

By prudently controlling and denying access of foreign (State) aircraft to their national airspace, States can control radio receivers and transmitters onboard these aircraft[135] and thus have (limited) control over possible cyber interference originating from foreign (State) aircraft. This control is limited, especially for States with small territory, because of possible cross-border radio spill-over: aircraft may fly ISR missions outside national territory but aimed at facilities and information inside this territory. In this case another legal limitation applies: harmful radio interference must be avoided.[136] The avoidance of harmful radio interference does not *per se* prohibit the transmission of radio signals, but aims to avoid radio interference or radio disturbance of other stations and services. The principle of the avoidance of harmful radio interference is not intended to protect information transmitted by radio, but to protect the radio spectrum itself, for example, against jamming.

131 Special authorisation for ISR in national airspace may be given by the over-flown State in case of military exercises or allied missions of air forces.

132 Even military transport aircraft of the European signatory States using foreign airspace under the *Diplomatic Clearance Technical Arrangement* (signed on 19 December 2012 under the auspices of the European Defence Agency) have to put any type of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) and/or Electronic Warfare (EW) equipment as well as Defensive Aids Sub Systems in 'OFF', 'INACTIVE', 'SAFE' or 'STAND-BY' mode.

133 Article 39(1)(c) of the *United Nations Convention on the Law of the Sea* (UNCLOS), 1982, 1833 U.N.T.S. 397.

134 *Ibid,* Article 19(2)(k).

135 Limitations apply also to aircraft radio equipment of civil aircraft, see Article 30 Chicago Convention, *op. cit.* note 6.

136 Article 45(1) of the *Convention of the International Telecommunication Union* (ITU), 1989, 1825 U.N.T.S. 390: 'All stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations.'

5. Conclusions

At present, cyber threats and cyber interference do not pose an imminent risk to aviation. Nevertheless, connectivity of aircraft flight controls and ATM, and the use of COTS components and software are on the rise. Safety-relevant aircraft systems and ATM will become increasingly vulnerable to outside cyber interference by State and non-State actors. Aviation security is the responsibility of States, and it is their responsibility to timely establish all regulatory measures for civil aviation to protect it against unauthorised cyber interference. Cyber security has come to the attention of ICAO, but to date, principles, standards and recommended practices are not established. As a starting point it is proposed that States should:

- make cyber security part of the airworthiness certification;
- adopt an anticipating regulatory approach to cyber security in aviation;
- avoid commercial off-the-shelf products for aviation safety-critical functions;
- limit and secure network interconnection for aircraft systems;
- find special solutions for interconnection in ATM; and
- ensure redundancy and diversity of radio navigation systems.

It may be comforting though that the legislative framework developed by States regarding criminal or private liability is solid enough to meet the new challenges posed by the cyber age. The existing international and national criminal law regimes cover malicious acts that lead to death, injury and damage, regardless of whether they are caused by cyber interference or conventional means. Likewise, the private liability regimes, most notably the Warsaw system, were established with great farsightedness to protect passengers and innocent bystanders on the ground against the typical risks of aviation, irrespective of the root cause of the disaster and whether it can be attributed to an identifiable perpetrator.

The status of military aviation and its use of national airspace during peacetime is completely different to civil aviation. Military aircraft are used for defensive and offensive purposes, and the same applies to cyber activities, which are intended to support or protect against missions of military aircraft. Numerous defensive and offensive cyber activities are conceivable. They have the potential to shape future air force operations during peacetime, ranging from export controls to electronic methods of air policing and new techniques for airborne ISR missions. The avoidance of harmful radio interference is one of the main legal limitations on military peacetime operations.

*Martha Mejía-Kaiser**

Space Law and Unauthorised Cyber Activities

1. Introduction

This chapter addresses the introduction, modification or destruction of software related to space systems, which include both the terrestrial segments and the space segments. Following a brief discussion of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies* of 1967[1] (Outer Space Treaty) and the *Convention on International Liability for Damage Caused by Space Objects* of 1973[2] (Liability Convention), possible scenarios of cyber activities intended to disable, destroy or manipulate space systems to cause damage are analysed in the context of these treaties. Legal rules are proposed to remedy the shortcomings of existing law when destructive cyber activities intrude into space systems.

2. Gateways for Cyber Activities

There are no internationally agreed legally binding definitions of 'cyberspace', 'cyber attack' or other related terms. Descriptions of this environment and the activities performed therein are presently being discussed in the military and academia. Nevertheless, some definitions used by the United States (US) military may be useful to show the complexity of this topic.

According to the Memorandum from the US Deputy Secretary of Defense, 'cyberspace' is defined as the '[g]lobal domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.'[3] It follows that a 'cyberspace operation', as defined by the US Department of Defense, is '[t]he employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace.'[4] Although

* This chapter represents the personal opinion of the author and should not be attributed to any organisation with which she is affiliated.

1 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, entered into force Oct. 10 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

2 *Convention on International Liability for Damage Caused by Space Objects*, entered into force Oct. 9 1973, 24 U.S.T. 2389, 961 U.N.T.S. 187.

3 Memorandum from the US Deputy Secretary of Defense, The Definition of Cyberspace, May 12, 2008, quoted in Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, The Air Force Law Review, vol. 68, 174 (2012).

4 Defense Department Cyber Efforts: Definitions, Focal Point and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates, US Department of Defense, Memo CM-0477-08 (2011)

this definition mentions only the achievement of 'military' objectives, it is obvious that cyber activities are not restricted to the military, but may be performed by other States' agencies and private actors, including companies, groups, and individuals.

Cyber activities can have defensive or offensive purposes. Defensive cyber activities include upgrading or restoring a computer system that has been damaged; investigating damage in the computer system; and maintaining situational awareness of own or allies' computer systems and networks. Offensive cyber activities are the insertion of computer programs into computer systems to observe and/or collect transmitted information; the disruption, degradation or destruction of the software of a system; the destruction of the hardware of a system; and the manipulation of a computer system to use it to cause further damage. US officials have indicated that offensive cyber operations should allow the military '[…] to [avoid using] kinetic tools',[5] but this does not mean that the effects of cyber activities are limited to manipulations of computer software. Although the word 'cyber' implies the introduction, modification or destruction of computer software, its effects can manipulate connected devices and release dangerous kinetic energy. As a US official said, '[…] cyber tends to mean anything that involves a network.'[6] In the specific case of cyber activities performed on space systems, damage may affect ground-based infrastructure or systems in outer space, or it may disrupt the communication links between the two.[7]

Damaging cyber activities can be performed without the authorisation of owners and operators of the space system, who may be governmental institutions, international organisations, private companies that own a satellite, or entities contracted to operate a satellite. Unauthorised cyber activities against a space system can enable the perpetrator to:

- exploit satellite[8] information without authorisation (e.g., accessing of and/or collecting information);
- disrupt the transmission of information by degrading or modifying it;
- partially damage or completely destroy a satellite's computer software and hardware (e.g., by introducing software viruses);

http://www.gao.gov/assets/100/97674.pdf, http://www.gao.gov/assets/100/97675.html.

5 Statement of US Official Erik Rosenbach, cited in Cheryl Pellerinn, *Cyber Operations Give Leaders new Options, Official Says*, American Forces Press Service, Apr. 12, 2012, http://www.defense.gov/News/NewsArticle.aspx?ID=67918.

6 *Id*.

7 John Leyden, *Inside the Mysterious US Satellite Hacking Case,* The Register, 21 Nov. 2011, http://www.theregister.co.uk/2011/11/21/us_sat_hack_mystery/.

8 Here the word 'satellite' will be used as a synonym of 'space object'.

- manipulate the command and control of a satellite (e.g., attitude control[9] and orbital trajectory), possibly causing collisions, explosions, atmospheric re-entry, depletion of limited satellite resources or third party damage.

As a technical countermeasure, computer systems at ground stations can be segregated by air-gapping, which is '[…] a measure undertaken to create a secure computer network by isolating it from insecure networks (such as the public internet) both physically and electromagnetically.'[10] If the system is perfectly segregated, non-authorised software (malware) can be introduced at a ground station only through the unauthorised use of portable flash drives (e.g., Universal Serial Bus – USB). The development of wireless technologies may allow unauthorised cyber activities to cross the air gap and render segregated systems vulnerable in the near future.

In 2008, the international press reported that the environmental remote sensing satellite-system of the US National Aeronautics and Space Administration (NASA) Earth Observing System had been accessed without authorisation through the internet. It was claimed that 'control' of the satellite was disrupted twice that year for several minutes. The ground station's operator, Kongsberg Satellite Services, a commercial entity incorporated in Norway that provides orbit support to 80 satellite systems from many countries and international organisations,[11] denied the occurrence of such events.[12] The operator of the ground station in Spitsbergen, Norway, said that

> The internet is occasionally used for distribution of x-band payload data received from the satellites to the end user. Hence, this communication channel cannot be an access point for unauthorized access if it had happened. Due to the layout of our communication systems it is not possible to access any NASA satellites from KSAT [Kongsberg Satellite Services] sources.[13]

The question remains if non-authorised access was gained and, if so, if the system was air-gapped at all or if it was believed to be protected by a series of firewalls that failed.

Unauthorised cyber activities can also disrupt the information flow from satellites' payload systems[14] to boycott not only civilian but also military operations. During Operation 'Desert Storm' in 1991, three hackers from the United Kingdom (UK)

9 See definition of 'attitude control' *infra* note 36.

10 Mudrinich, *supra* note 3, at 198.

11 Satellite services are provided, among others, to US Iridium, European Space Agency's Sentinel and European Union's Galileo.

12 John Leyden, *supra* note 7.

13 John Leyden, *supra* note 7.

14 The term 'payload' is used to indicate the device that serves the main mission of the satellite, e.g., communications satellites have a communication payload which is comprised of '[…] communication transponders, antennas and associated equipment involved directly in the receipt and transmission of radio signals from and to the earth station network'. ITU, Handbook on Satellite Communications, 381 (2002). In addition to the payload(s), most satellites have flight control electronic systems. Both, payloads and flight control systems are controlled by onboard computer systems. See section 4.1.1 of this chapter.

accessed a secure military computer system over the internet and manipulated it to disrupt incoming satellite weather data before the invasion of Iraq

> […] by breaking the codes and inserting their own data […] to slow down the split-second rate at which the computer received weather pictures form the satellites in outer space. This action effectively threw the whole system out of synchronisation and gave a totally inaccurate advance picture of the weather conditions expected in the Gulf region.[15]

Original plans for the invasion had to be modified. The perpetrators were identified and were prosecuted under the UK *Computer Misuse Act*.[16]

Other gateways for cyber activity to a space object's flight control system and payload are the radio communication links. In 1986, the satellite channel Home Box Office (HBO) changed its commercial scheme by scrambling[17] its direct broadcast signals. Customers were required to pay a fee and to buy a device to unscramble the signal. A TV satellite dish dealer, whose business was harmed by HBO's new policy, was also a technician at a ground station servicing other satellite systems. He pointed an antenna to the Galaxy-1 satellite that served HBO and sent a powerful signal.[18] With his uplink signal he transmitted his own message instead of the HBO movie for about five minutes to HBO customers.[19] Given that large antennas are needed to transmit a signal to Galaxy-1 in the geostationary orbit[20] at 36,000 km altitude, investigators could pin-point the origin. The perpetrator was identified and fined US$5,000. In other cases, radio transmitters have been briefly positioned close to a satellite transmitter station to hack the uplink signal. For example, in 1990, a US citizen hacked the satellite signal to replace a pornographic channel with a religious one. 'The perpetrator was convicted of intentional interfering with a communications satellite broadcast and operating a satellite up-link transmitter without authorisation.'[21]

---

15 Michael Potter, The Outer Space Cyberspace Nexus: Satellite Crimes, in IISL Proceedings, 94-IISL.1.822, 9-10 (1994). Stern Chester, Hackers' threat to Gulf War Triumph; Trio Played Havoc with Weather Computer Before Iraq Attack, in Mail on Sunday, (Mar. 21, 1993) at 15, cited in Michael Potter. Different conditions of spoofing have been studied just before signals are sent to a geostationary satellite by using a satellite connection to the internet. Results of one of these studies is presented by Joseph Ishac and Mark Allman, On the Performance of TCP [Transmission Control Protocol] Spoofing in Satellite Networks, IEEE Milcom, Oct (2001), http://icir.org/mallman/papers/milcom01.pdf.

16 Michael Potter, *supra* note 15.

17 'Scrambling' is the insertion of a quasi-random signal to the main signal to make it illegible to simple radio receivers. The main signal may be cleaned though special radio receptor devices.

18 David Harland and Ralph Lorenz, Space System Failures, 237 (2005).

19 The following message appeared: 'Good Evening BHO. From Captain Midnight. $12.95 a month? No Way! (Showtime/The Movie Channel beware).' Harland & Lorenz, *id.*, at 238. The perpetrator, John R. MacDougall, gives an account of the event at the following site: http://www.textfiles.com/100/captmidn.txt.

20 See explanation of Geostationary Orbit *infra* note 28.

21 *Virginia Man Sentenced for Satellite Interference*, in Space News, (Dec. 17-23, 1990), cited in Michael Potter, *supra* note 15, at 7.

These cases show that access to space systems' payloads and flight control systems can be achieved without use of the internet when unauthorised cyber activity is transmitted through a more powerful signal that overrides the electromagnetic signals of the operator.

In order to understand the legal ramifications of unauthorised cyber activities affecting space activities, a brief look at international space law is necessary.

3. A Brief Look at Space Law

After the launch of the first space object in 1957, it became evident that this activity would bring about new challenges and impact the whole international community. It was feared that outer space activities such as observation of military capabilities or natural resources could be detrimental to some States, and that outer space could become a new arena of armed conflict. Launch failures raised the concern that uncontrollable space objects could reach the other side of the planet in a matter of minutes and cause vast damage.

Several States addressed these issues at the United Nations (UN). The UN General Assembly established the 'Committee on the Peaceful Uses of Outer Space' (COPUOS),[22] which was given the mandate to develop guidelines for the peaceful use and exploitation of outer space. Also, by placing the first space object in outer space in 1957, the use of radio electromagnetic signals went beyond the limits of ground-based communications. This moved the UN General Assembly in 1961 to recognise that there was a need for 'effective operational satellite communication'[23] and it encouraged the International Telecommunication Union (ITU), which had already planned to address space communications in a conference, to maintain such work and cooperate with COPUOS and other UN organs and organisations.[24]

Thus regulation took two parallel paths. COPUOS served as a forum for the elaboration and adoption of five multilateral treaties and UN General Assembly resolutions establishing legal principles for space activities,[25] which became the roots of 'space

22 COPUOS was first established as *ad hoc* committee in 1958, but in 1959 it was granted permanent status. Francis Lyall and Paul Larsen, Space Law, A Treatise, 18 (2009).

23 UN GA Res. 1721 (XVI), on International Co-operation in the Peaceful Uses of Outer Space, (1961), Part D.

24 *Id*.

25 Outer Space Treaty, *supra* note 1; Liability Treaty, *supra* note 2; *Convention on Registration of Objects Launched into Outer Space*, entered into force Sept. 15, 1976, 28 U.S.T. 695, 1023 U.N.T.S. 15; *Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched Into Outer Space*, entered into force Dec. 3, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 119; *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, entered into force July 11, 1984, 1363 U.N.T.S. 3. Five important UN Resolutions of the General Assembly on space activities are: The Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, UN Doc. A/RES/18/1962 (1963); The Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, UN Doc. A/RES/37/92 (1982); The Principles Relating to Remote Sensing of the Earth from Outer Space, UN Doc. A/RES/41/65 (1986); The Principles Relevant to the Use of Nuclear Power Sources in Outer Space A/RES/47/68

law' as a new branch of public international law. Correspondingly, the ITU established regulations and procedures for space communications, which became part of the already existing 'telecommunications law'.

3.1 Regulation of Space Communications

Electromagnetic signals can be transmitted by wired or wireless networks. Wireless signals are also known as radio communication. Communications links between the Earth and a space object are established by such radio communication. An electromagnetic signal is the 'horse' that carries information (e.g., 1,000 simultaneous telephone calls in one carrier signal). In the course of several conferences, the ITU allocated frequencies[26] for radio satellite services, developed rules for the use of radio frequencies by space objects and rules for orbital positions[27] in the Geostationary Orbit.[28] For the assignment of frequencies, operator States of space systems may enter anticipated frequencies within the corresponding allocation into the 'Master International Frequency Register'[29].

The increasing number of space objects and the need to communicate efficiently with such objects necessitated the rational use of the available radio electromagnetic frequencies to avoid harmful interference.[30] In 1959, the ITU started to devote attention

(1992); The Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries, UN Doc. A/RES/51/122 (1996). Other space related UN Resolutions and legal instruments until 1999 are listed in this UN Document: International Agreements and other Available Legal Documents Relevant to Space-Related Activities (1999), http://www.oosa.unvienna.org/pdf/spacelaw/intlagree.pdf.

26 For the rational and efficient use of the radio-frequency spectrum the ITU has divided the radio-frequency spectrum into 'bands' and allocated them to specific uses (e.g., satellite earth to space, satellite space to earth, inter-satellite communications, meteorological satellites). Frequency Sharing, at 815 & 914, ITU, Handbook on Satellite Communications, *supra* note 14, at 9. The ITU has also divided the world into three regions for the allocation of frequencies, ITU, Frequency allocations, Radio Regulations Article 5.2., http://life.itu.int/radioclub/rr/art05.htm.

27 Space Law, Basic Legal Documents (Böckstiegel, Benkö and Hobe eds., 2012), vol. 3, C.IV, ITU, at 2.

28 The Geostationary Orbit (GEO) is a three dimensional circular area (with the shape of a ring) at about 36,000 km altitude parallel to the Earth's equator. GEO functional space objects move from west to east and take 24 hours to complete one orbit. This movement is harmonized with the Earth's rotation, so that the objects seem to be 'stationed' in a particular point above the equator, thus antennas on Earth do not need to find and follow a fast moving satellite. Transmitting antennas need to be powerful enough to send a signal to 36,000 km distance. Martha C. Mejía, La Órbita Geoestacionaria, Instituto de Geofísica, UNAM, Comunicaciones Técnicas No. 1 (1987).

29 The Master International Frequency Register is administered by the Radiocommunication Sector, a permanent ITU organ. Francis Lyall, *The International Telecommunication Union: A World Communications Commission?* Proceedings of the Colloquium on the Law of Outer Space, IISL.1.-94-817, 43 (1994). The Radiocommunication Sector was created (1993) with the aim '[…] to ensure national, equitable, efficient and economical use of the radio-frequency spectrum and satellite orbits.' ITU, Handbook on Satellite Communications, *supra* note 14, at 815. Today the principal legal instruments of this organization are the Constitution, the Convention and the Administrative Regulations, see Lyall & Larsen, Space Law, *supra* note 22, at 206.

30 Electromagnetic 'harmful interference' is defined by the ITU as '[i]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations'. Annex to ITU Constitution, Definition of Certain Terms Used in this Constitution, the Convention and the Administrative Regulations of

to the coordination of space telecommunications for the avoidance of such interference.[31] This cardinal principle of radio communications is spelled out in Article 45 of the ITU Constitution[32] (197, PP-98), which also applies to space radio communications:

> All stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations. […] Member States recognize the necessity of taking all practical steps to prevent the operation of electrical apparatus and installations of all kinds from causing harmful interference to the radio services or communications mentioned.

Although Article 45 prohibits harmful electromagnetic interference, it does not prohibit unauthorised cyber activities. The ITU only regulates the use of the radio frequencies, but not the information transmitted.

3.2 Responsibility for Performing Space Activities

Of the five treaties that were negotiated in the framework of the UN, the Outer Space Treaty of 1967 and the Liability Convention of 1972 are of relevance in the context of malicious cyber activities. The Outer Space Treaty was the first international space law instrument to be adopted. It has been ratified by more than 100 States,[33] including all space-faring nations. The Outer Space Treaty lays down the basis of space law. In Article III it stipulates:

> States party to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.

The drafters did not provide a list of what constitutes 'activities in the exploration and use of outer space', but given the time at which it was written it is not likely that they contemplated software issues or cyber activities at all.

---

the International Telecommunication Union. No.1003. Also interplanetary space objects travelling in space or on the surface of celestial bodies need communication links free of harmful interference.

31 In 1959, the ITU held a World Administrative Radio Conference in Geneva, where definitions related to space activities were agreed. Lyall and Larsen, Space Law, *supra* note 22, at 200.

32 ITU Constitution is available at http://www.itu.int/dms_pub/itu-s/oth/02/09/s02090000115201pdfe.pdf.

33 By 2013, the Outer Space Treaty has been ratified by 102 States. See United Nations Treaties and Principles on Outer Space and Related General Assembly Resolutions. Status of international agreements relating to activities in outer space as of 1 January 2013, http://www.unoosa.org/oosa/en/SpaceLaw/treatystatus/index.html.

Important to note, the Outer Space Treaty introduced a new norm unprecedented in public international law: the responsibility of States for any national activity in outer space. Article VI of the Outer Space Treaty states:

> States Party to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities […] the activities of non-governmental entities […] shall require authorization and continuing supervision by the appropriate State Party […].

Thus it is the 'primary international responsibility' of States to authorise and continuously supervise the space activities of their governmental and non-governmental institutions.[34] In case of violation of such duties or the occurrence of damage, even if there is no breach of a norm, such States bear a 'secondary international responsibility', to respond the international community through '[…] payment of compensation, an apology, the punishment of the individuals responsible'[35] and other means.

Although cyber activities were not considered when the international space law instruments were drafted, their legal effect needs to be explored in the event that unauthorised cyber activities against space systems cause damage.

4. Liability for Damages Caused by Cyber Activities

Damage caused by cyber activities can be diverse. The manipulation or deletion of authorised software or the introduction of malware in a space system can impact satellite transmissions of commercial, scientific, military and other information with subsequent effects on dependent operations on Earth. It is not possible to draw up an exhaustive list of scenarios, but they can be grouped in those related to (1) loss of service and the space object and (2) physical damage to other space objects in outer space or on the Earth's surface.

4.1 Loss of Service and Operational Life and Destruction of Space Objects

A cyber activity could be directed against the controls of space objects, with effects that can range from the loss of signal and service to the destruction of the space object. Before discussing the Liability Convention it is necessary to address some technical issues that may help to understand the vulnerable aspects of space systems.

---

34 The concept 'non-governmental' of Article VI of the Outer Space Treaty '[m]ay reasonable be construed to include private firms […]'. Nicolas Matte, Space Activities and Emerging International, 297 (1984).

35 Ian Brownlie, Principles of Public International Law, 442 (6th ed. 2003).

4.1.1 Technical Background

Most satellites are characterised by a set of six subsystems plus the payload:

- structure;
- thermal control system (keeps an adequate temperature in the extreme space environment to protect devices);
- power system (solar panels that gather the Sun's energy or nuclear power sources and batteries that store such energy),
- attitude control system[36] (including propulsion with fuel tanks, sensors, actuators);
- telemetry, tracking and command system[37] (consisting of on-board computer, radio receivers/transmitters and antennas); and
- harness (the cables that connect the devices).[38]

These six subsystems are usually referred to as the 'satellite bus'. The seventh subsystem is the payload.[39] The satellite is controlled via the Telemetry, Tracking and Command System that directs the ground station's commands received by the satellite to act on the various devices. Depending on the mission, there can be a single ground station or several stations spread around the globe for a better coverage. The ground stations may collect housekeeping data from the bus telemetry and/or data from the payload.

Each space object has one or several 'radio stations' on board.[40] Some support the flight control of the satellite,[41] while others are used for different types of payload depending on the mission of the satellite, for example, communication, remote sensing or navigation. A space object may have several computer systems that serve either the flight control

36 A satellite's 'attitude control' is necessary to maintain the '[…] antenna radio frequency beam pointed at the intended areas'. Attitude control also serves to align sensors and other instruments in a certain orientation, in order to perform certain tasks as the gathering of remote sensing data from Earth's surface, etc. Such attitude control is achieved '[…] through the use of small jets [e.g., venting gases], magnetic torquers or altering the position of "solar sails"', see 6.2.4.2. Attitude Control, ITU, Handbook on Satellite Communications, *supra* note 14, at 369-370.

37 'Tracking' means '[…] sending a ranging signal to […] and from […] the satellite. This signal is processed […] for […] relocating the satellite'. 'Telemetry' is the collection and transmission of data of '[…] sensors distributed throughout the spacecraft'. 'Command' are the '[…] signals […] transmitted from the [ground stations] to the satellite to satisfy operational mission requirements or to respond to emergency conditions', see 6.2.6. Telemetry, command and ranging, ITU, Handbook on Satellite Communications, *supra* note 14, at 377. See also US Army Reference Text, Chapter 7 Satellite Systems, http://www.fas.org/spp/military/docops/army/ref_text/chap07a.htm.

38 Felix Huber, Deutsches Zentrum für Luft- und Raumfahrt (DLR, German Space Agency), personal communication with the author, 9 October 2013.

39 On the term 'payload', see *supra* note 14.

40 Perek explains that 'space radio receivers and transmitters', maybe a relative small part of a satellite. Several of these radio stations '[...] may be mounted on the same satellite.' Perek L., *Rational Space Management*, in ZLW, Nr. 53, 575-576 (2004). 'Space station' was defined in the World Administrative Radio Conference in Geneva in 1959. Lyall and Larsen, Space Law, *supra* note 22, at 200.

41 Operations of the Tracking, Telemetry and Command system, Attitude Control system and other systems form together the 'flight control' of the satellite.

system or the control of payloads. If a space object has multiple payloads, each will have its own computer systems to serve its particular mission. Remote sensing payloads have computer systems that control the sensors to collect and store data for transmission, either immediately to ground stations within view, or at a later time.[42]

Satellites with communications payload also have on-board computer systems. Such satellites are fitted with 'transponders' which are radio receivers and transmitters assembled in pairs.[43] With the use of multiplexing technology, each transponder may route hundreds of simultaneous telephone calls or several television channels within one single electromagnetic carrier signal. Transponders may be leased to institutions of the State that owns the space object or to foreign public or private institutions. Thus several users can exploit one single space object. Today 'small telecommunication satellites' have 24 transponders, and 'large satellites' may have around 50. Currently the annual average profit for one commercial transponder is about US$2 million.[44]

Many operational space objects are several years old and their on-board computer systems are not robust enough to withstand interference from more recent computer viruses or other unauthorised software. Although on-board software may be updated from the ground, the aging computer hardware limits the complexity of updates, rendering an aging satellite computer system increasingly vulnerable to unauthorised cyber activities.

On Earth, security of ground stations and encryption[45] of satellite signals depends on the level of sophistication and age of the systems. Unsecured ground stations and non-encrypted signals are highly vulnerable to unauthorised interference, manipulation or deletion of software or introduction of malware. Unauthorised individuals or institutions may take advantage of the infrastructure necessary to command and control a satellite.

---

42 Optical remote sensing satellites relay data temporarily stored in the onboard computer to specific Earth stations when passing them on each satellite's orbit. Radar remote sensing satellites generate an enormous amount of digital data that cannot be stored onboard. This data needs to be sent to Earth stations within the sight of the satellite as soon as it is produced. Ferrazzani M., *Remote Sensing, General Principles and ESA Policy*, Proceedings of the Third ECSL/Dutch NPOC Workshop, Noordwijk, Apr. (1994), at 13. Although radar data are not stored on board the satellite, a computer system is an important element of the remote sensing payload for the fulfillment of the data gathering task.

43 See 2.1. Characteristics of a satellite link, ITU, Handbook on Satellite Communications, *supra* note 14, at 41. Each transponder receives radio electromagnetic signals (up-link), transforms them into another frequency, amplifies their power and sends them back to Earth stations (down-link). The frequency has to be converted in order to avoid interference with the incoming signal.

44 Robotic Geostationary Orbit Restorer, Final Report-Executive Summary, EADS Space Transportation, 1 (2003).

45 Encryption is '[t]o alter information using a code or mathematical algorithm so as to be unintelligible to unauthorized readers'. The Free Dictionary, http://www.thefreedictionary.com/encrypt.

4.1.2 Possible Scenarios

The vulnerabilities of space systems, ground stations and radio communications could result in the following scenarios of cyber interference:

- A satellite's attitude control could be altered so that communication antennas do not point to ground stations, leading to loss of remote sensing, communication or navigation services.
- A satellite's payload systems could be manipulated to render them useless.
- A satellite's radio communication links for flight control or payload systems could be interrupted, manipulated or eavesdropped.
- The flight control of a satellite could be manipulated to change its orbit, leading to loss of communication or, in case of a navigation satellite, loss of the required precision of service.
- Satellite control systems could be manipulated so that the fuel for station keeping and energy for attitude control are wasted, leading to a reduction or loss of the remaining operational lifetime of a satellite.
- A satellite in a low orbit could be de-orbited[46] to prematurely re-enter the Earth's atmosphere, leading to its destruction and the corresponding loss of the satellite and its service.
- Satellites that have self-destruction mechanisms[47] (some military satellites) could be manipulated to explode in orbit.
- Satellites that have been abandoned in outer space and are considered space debris[48], but still possess intact payload systems (e.g., communications payload), could be misused by unauthorised parties.

46 See 3.4.2. Definition of 'De-Orbit': '[…] intentional changing of orbit for re-entry of a space system into the Earth's atmosphere […] by applying a retarding force, usually via a propulsion system'. Inter-Agency Space Debris Coordination Committee (IADC), Space Debris Mitigation Guidelines, UN Doc. A/AC.105/C.1/L.260 (2002).

47 'On 6 Dec. 1991 Kosmos 2163, a maneuverable Soviet spacecraft which had been in orbit for 58 days, experienced a major breakup at an altitude of approximately 210 km. Although numerous pieces of debris were created, the fragments decayed rapidly leaving no long-term impact on the near-Earth environment. The assessed cause of the event is the deliberate detonation of an explosive device'. The Fragmentation of Kosmos 2163, study prepared by Teledyne Brown Engineering for NASA Lyndon B. Johnson Space Center, (Jan. 1992), http://archive.org/stream/nasa_techdoc_19940012030/19940012030_djvu.txt.

48 'Space debris' objects are defined by the IADC as '[…] all man-made objects including fragments and elements thereof, in Earth orbit or re-entering the atmosphere, that are not functional.' Definition of 'space debris', IADC Space Debris Mitigation Guidelines, *supra* note 46.

4.1.3 The Liability Convention and Loss of Service or Destruction of Space Objects

The Liability Convention is the special space treaty that addresses damage and compensation.[49] As the name of the Convention indicates, this treaty applies only to damage caused by space objects. Article 1(a) states: 'For the purposes of this Convention […] [t]he term "damage" means loss of life, personal injury or other impairment of health; loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations […].' Article 1(d) defines 'space object' as follows: 'The term "space object" includes component parts of a space object as well as its launch vehicle.'

This Convention applies to damage which arises from the kinetic energy and other physical direct damages that unfold following a collision by the space object's body or parts thereof.[50] For that reason, damages directly caused by unauthorised cyber activities to a space object are not covered by the Liability Convention *per se*. Unauthorised cyber activities against space systems can also not be considered as space activity under Outer Space Treaty Articles III and VI. In conclusion, the State of the satellite owner or operator who has suffered a loss of satellite service and a loss of the space object itself, does not receive any compensation under the terms of the Liability Convention from the State of nationality of the perpetrator who performed the damaging cyber activity.

4.2 Physical Damage Caused by Space Objects in Outer Space or on Earth

Kinetic or other kinds of physical damage caused by space objects after an unauthorised cyber activity would have a different outcome under the Liability Convention. Before discussing the Liability Convention, it is necessary to look at the technical background.

4.2.1 Technical Background

All man-made objects in outer space are in movement. At present there are about 1,000 operational satellites of developed and developing States in Earth orbit.[51] From the moment an object is launched into outer space it obtains immense kinetic energy through its acceleration. All objects assembled to the launcher also bear this kinetic energy. Such objects will keep this kinetic energy due to inertia as long as they stay

---

49 By 2013, the Liability Convention has been ratified by 89 States. See UN Status of International Agreements relating to Activities in Outer Space, *supra* note 33.

50 According to Smith and Kerrest, 'The formulation underlines that the damage must be caused by the space object itself and not by the product/application emanating from its operation.' Smith & Kerrest, Article I, Liability Convention, in Cologne Commentary on Space Law (Hobe, Scmidt-Tedd & Schrogl, eds. 2013), vol. 2, at 111.

51 ESA/ESOC, Space Debris Evolution in Pictures, available at: http://www.esa.int/About_Us/ESOC/Space_debris_-_evolution_in_pictures.

in outer space and also in the event that they survive atmospheric re-entry and reach the Earth's surface. However, most space objects re-entering the Earth atmosphere disintegrate because of atmospheric friction.

Valuable space objects, like manned space objects, re-enter in a controlled manner. Space objects that have completed their operational life and which may survive atmospheric re-entry due to their materials or size[52] are usually de-orbited with a controlled splash-down in an ocean or landing in a non-inhabited area to avoid casualties and other damage. However, there have been cases of objects not totally disintegrating on re-entry and reaching populated areas.[53]

Besides the kinetic energy of space objects maintained by inertia, other energies are stored in a space object, including fuel, pressurised gases and electricity. All these energies can be controlled from ground stations. If such stored energy is released in a violent way, such as by an explosion following a collision with another object, each piece of the space object is charged with this additional kinetic energy.

Some space objects have power sources on board with nuclear materials, like Uranium or Plutonium, to supply the electrical devices on board with energy.[54] Although the amount of radioactive materials on board satellites is relative small,[55] there is a risk of radioactive contamination should an accident occur during launch or when the space object survives re-entry and reaches the Earth's surface.[56]

---

52 Uncontrolled de-orbiting is possible with satellites of less than 20 kg, because they completely melt during re-entry, unless they do consist of hard metals, see International Academy of Astronautics (IAA), Position Paper on Space Debris Mitigation, 24 (2005), http://iaaweb.org/iaa/Studies/spacedebrismitigation.pdf. According to ESA space debris specialist Klinkrad, 20% to 40% of large space objects which enter the atmosphere in an uncontrolled manner are not destroyed by friction and reach the surface of the Earth. Manfred Lindinger, *Kampf gegen Weltraumschrott, Wir haben unsere Warnschüsse gehabt*, FAZ (Apr. 22, 2013), http://www.faz.net/aktuell/gesellschaft/umwelt/kampf-gegen-weltraumschrott-wir-haben-unsere-warnschuesse-gehabt-12158437.html.

53 One of these events is the tragic destruction of the US Space Shuttle Columbia in 2003. The pieces were disseminated in a vast area in the United States. Chris Bergin, *NASA Managers Discuss Fragmentation Risks as UARS Heads Back to Earth*, NASA Spaceflight.com, 2011, http://www.nasaspaceflight.com/2011/09/nasa-managers-fragmentation-risks-uars-heads-back-earth/. In 1991, the Russian Salyut-7 re-entered Earth's atmosphere and several fragments reached the town Captain Bermudas, near Buenos Aires, Argentina. No casualties or other damages were reported. Lyall & Larsen, Space Law, *supra* note 22, at 118. Upcoming and recent space debris atmospheric reentries are available at the following website of Aerospace Corporation: http://www.aerospace.org/cords/reentry-predictions/upcoming-reentries/.

54 Radioactive materials used as nuclear power sources (NPS) for the generation of electricity are Plutonium-238 and Uranium-235. Gary Bennet, *Space Nuclear Power*, Encyclopedia of Physical Science and Technology, vol. 15 (2002). About half of the US space objects with NPS are in Earth orbits. The rest are onboard interplanetary space probes: Voyager, Cassini, New Horizons, etc., *id*., at 543.

55 The Soviet Cosmos 954 that crashed on Canadian territory in 1978 carried approximately 23 kg of Uranium-235. Gary Bennett, *A Look at the Soviet Space Nuclear Power Program*, NASA, Energy Conversion Engineering Conference (1989), at 1191.

56 Bennett reports on reentries of Soviet space objects with NPS, *id*. Some Soviet and US space objects with NPS that terminated their functional life have been transferred to 'Nuclear Safe Orbits' (NSO) at altitudes where space objects will take 300 years or more to naturally decay and re-enter Earth's atmosphere. Bennett, *Space Nuclear Power, supra* note 54, at 541-542.

Some satellite owners and operators decommission[57] their space objects without powering down systems and without performing other 'passivation' measures. Passivation is '[…] the elimination of all stored energy on a space system […]. Typical passivation measures include venting or burning excess propellant, discharging batteries and relieving pressure valves before shutting-off the space object.'[58] This measure is recommended by the Inter-Agency Space Debris Coordination Committee (IADC) in its Space Debris Mitigation Guidelines, to diminish the potential of break-ups in outer space. Most space objects that are decommissioned start tumbling and cannot point their antennas. Despite this, there are some intact satellites that have been abandoned in outer space and have been misused, as is the case with disused but not 'passivated' US Navy communications satellites which have been used by unauthorised persons.[59]

4.2.2 Possible Scenarios

Taking into consideration the kinetic and other energy on board space objects, and the possible cyber manipulation of their flight controls, the following damage scenarios may, either now or at some future date, occur:

- The flight controls of an operational space object or a decommissioned but serviceable space object (with still intact flight control and fuel remnants that may allow reactivation) could be manipulated to collide with other space objects.[60]
- A satellite in low Earth orbit could be de-orbited to enter Earth's atmosphere. If it survives atmospheric friction it may produce damage to aircraft in flight or on the surface of the Earth.[61]

---

57 Satellite owners and operators announce that they will declare a satellite as 'decommissioned' in order to inform users that the satellite will be deactivated. In some instances a new satellite takes over the work load. In an implicit way, satellite owners and operators declare such decommissioned space object as 'space debris'.

58 'Mitigation measures and related terms' and 4.1. 'Passivation', IADC Space Debris Mitigation Guidelines, *supra* note 46.

59 The US Navy launched the Fleet Satellite Communications System (FLTSATCOM) in the 1980's. These satellites were abandoned when a new space segment was placed in orbit. Two still operable obsolete FLTSATCOMs have unsecured telephone transmission systems that have been abused by drug dealers and other unauthorized persons. The only legal recourse to counter-act this has been arresting the persons (mostly in Brazil) that used the satellite transponders, but the satellites are still there open to be used by anyone. Marcelo Soares, *The Great Brazilian Sat-Hack Crackdown*, Wired (Apr. 20, 2009), http://www.wired.com/politics/security/news/2009/04/fleetcom?currentPage=all#. It is evident that the US Navy did not perform passivation measures (the batteries remained connected to the solar panels), so the batteries on board are still being recharged with solar energy, allowing the operation of transponders.

60 Although it may seem improbable at present that a space object is directed to collide with another space object through an unauthorized cyber activity in the Earth's orbital region, the day will come when the accuracy of conjunction assessments will improve to a degree to make a directed collision more probable.

61 Besides dangers resulting from kinetic energy, there are some space objects with nuclear power sources on board that may contaminate a crash location. Although the amount of such radioactive materials is relative small, and would not cause a catastrophic event of the magnitude of nuclear power station accidents on Earth, as Chernobyl and Fukushima, it may still cause personal injury and result in high cleaning costs. The Soviet Cosmos 954 satellite entered the atmosphere and exploded in 1978, contaminating a vast area of Canadian territory. C.A. Morrison, Voyage into the Unknown, the Search and Recovery of Cosmos 954 (1982). Other space objects with nuclear power sources that entered the atmosphere were the US Apollo 13's Service Module

- The navigation system of a launcher could be manipulated at the time of launch leading to a crash on the surface of the Earth at a random or a determined impact location.

All these scenarios have one common denominator: unauthorised seizure of space systems and their support elements, affecting flight control[62], the service of the payload(s), or both. To cause such damage, cyber activities could be directed against computer systems of ground stations and institutions supporting space systems or directly against the space segment by radio interference with communication links, overriding the authorised signal. If the communication system of a decommissioned satellite can be accessed by unauthorised persons,[63] there is also the chance that a space object can be seized through malware directly sent to a satellite using a powerful electromagnetic signal that overrides the original signal. Such cyber activity may enable the perpetrator to take control of the flight system and payload. For this kind of cyber activity, it is necessary that the satellite has a still functional Telemetry, Tracking and Command system, intact propulsion system and fuel remnants, and that the perpetrator possess specific knowledge on confidential information on satellite's hardware, command structure, signal frequency, modulation, data rate, etc.[64]

4.2.3 The Liability Convention and Damage in Outer Space

The Liability Convention addresses damage to a space object occurring in outer space. Article 3 of the Liability Convention states:

> In the event of damage being caused elsewhere than on the surface of the Earth to a space object of one launching State or to persons or property on board such a

that sank in the Pacific Ocean in 1970. See NASA, Apollo 13 Command and Service Modules, http://nssdc.gsfc.nasa.gov/nmc/masterCatalog.do?sc=1970-029A; the fuel core of the Soviet Cosmos 1402, which submerged in the Atlantic Ocean in 1983 and the Soviet Cosmos 1900. Bennet, *A Look at the Soviet Space Nuclear Power Program, supra* note 55, at 1192 & 1187. NASA reported that Cosmos 1900 sank also in the Atlantic Ocean in 1988. Chris Bergin, *supra* note 53. See also Andrea Gini, *Safety of Nuclear Powered Missions,* in Space Safety Magazine (21 Oct. 2011), http://www.spacesafetymagazine.com/2011/10/21/plutonium-power-source-considered-choice-type-deep-space-missions-extraordinary-scientific-results-missions-voyager-pioneer-apollo-nuclear-power-yet-senate-appropriations-committee-decided-fund-ad/. The NPS of Cosmos 1402 and 1900 re-entered uncontrolled, so it was a good luck that they did not crash in habited areas.

62 Flight control may be performed by other institutions than the satellite operator. For example, a satellite operator may contract a private company to perform orbital and attitude corrections, while other institution(s) engage exclusively in the day-by-day commercial telecommunication transmissions. Contracting out of these functions increases the number of involved parties, interfaces, communication links and vulnerabilities. Such institutions could also be subject of cyber activities that would hinder the communication of reliable satellite conjunction assessments to satellite operators; access could be denied to space segment rendering impossible any orbital correction; and finally information of space debris data bases may be partially or totally deleted or the information could be modified, provoking false conjunction assessments that lead to a collision of space objects in traffic areas with high collision risk.

63 As in the case of the US Navy FLTSATCOM satellites, see *supra* note 59.

64 Felix Huber, DLR, personal communication with the author, 9 October 2013.

> space object by a space object of another launching State, the latter shall be liable only if damage is due to its fault or the fault of persons for whom it is responsible.

According to Article 1(c) of the Liability Convention, '[t]he term "launching State" means: (i) A State which launches or procures the launching of a space object; (ii) A State from whose territory or facility a space object is launched.' With this treaty the signatory States accept a legal link with the space objects from the moment of their launch and admit responsibility for the inherent risks of charging them with kinetic energy and other dangerous energies.[65] They also accept liability for damages caused by such objects, and to pay compensation. Thus the launching State[66] is ultimately responsible[67] and liable, even if the damage physically caused by the space object is the result of unauthorised cyber activity.

However, according to Article 1(c) of the Liability Convention, liability for damage to other space objects in outer space requires proof of 'fault'. There are two ways to attest fault, by demonstrating either breach of a protective rule or an intentional or negligent act that caused the damage. At present there are no binding rules, like space traffic rules, that would protect other space objects with legally binding force. At international level there are only recommendations to limit the probability of accidental collision using orbital data and the application of avoidance manoeuvres; for example the UN Space Debris Mitigation Guidelines recommends in its Guideline 3 to limit the probability of accidental collision in orbit through the adoption of collision avoidance procedures.[68] Some States, including the US[69] and France,[70] have domestic law covering this subject.

---

65 The use of nuclear power sources in outer space is permitted. Some safety recommendations have been adopted by UN General Assembly Resolutions: Resolution Relating to the Information to be Furnished by States about the Malfunctioning of NPS in Outer Space, UN Doc. Resolution 33/16 No. 9 (1978); Principles Relevant to the Use of Nuclear Power Sources in Outer Space, UN Doc. A/RES/47/68 (1992); the following treaty could also be interpreted as to include accidented space objects with nuclear power sources: Article 1 (Scope of Application) of the *Convention on Early Notification of a Nuclear Accident*, done on Sep. 26, 1986, entered into force Oct 27, 1986, U.N.T.S. vo. 1439-I-24404. Smith & Kerrest note that damage arising from the use of NPS was not excluded by Outer Space Treaty and is therefore covered by the Liability Convention. Smith & Kerrest, *supra* note 50, at 112.

66 At the beginning of the space era it was no problem to identify the launching State. In the course of time, with increasing participation of States and international organization, it is becoming difficult to identify the launching State. However, this issue is not being addressed here.

67 Article VI of the Outer Space Treaty, *supra* note 1.

68 UN Space Debris Mitigation Guidelines, *infra* note 83.

69 In the United States, GEO satellite owners shall address in their license's application the measures to prevent collisions. *Code of Federal Regulations*, US Government Printing Office, cite 47 C.F.R. 25, Title 47-Telecommunication, vol. 2 (2004), § 25.114 (14).

70 Under the French legislation, space segment operators are required to submit a study on dangers of accidents due to external or internal causes, including the collision with a satellite in the Geostationary Orbit. *Arrêté du 31 mars 2011 relatif à la réglementation technique en application du décret n° 2009-643 du 9 juin 2009 relatif aux autorisations délivrées en application de la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales* (Fr), Article 32. Technical Regulations of the French *Space Operations Act*, last amended in 31 Mar 2011, www.iadc-online.org.

The second way to prove fault is to demonstrate intent or negligence on the part of the State with the legal link to the space object that caused the damage. Intent can be defined as '[the] desire to bring about [the] result that will invade [the] interests of another.'[71] Negligence can be defined as '[t]he failure to use such care as a reasonable prudent and careful person would use under similar circumstances.'[72]

In regard to intent, it is unlikely that a launching State would publicly admit having wilfully supported an act of cyber interference to its own space object by individuals or institutions from another State that resulted in further damage to third States. Concerning negligence, at the present state of technology, States are unprepared to react quickly to cyber activities because they lack standardised technological means to prevent and halt cyber activities on space vehicles. This would typically exonerate a launching State from liability for third party cyber interference under the Liability Convention. However, increasing cyber threats, growing cyber security awareness and more efficient technical countermeasures could lead to a different assessment in the future. A launching State could be held negligent if it fails to undertake reasonable actions to prevent or halt unauthorised cyber interference with its national space objects. Liability may arise on the grounds of negligence under the rule expressed in *The Corfu Channel Case*[73] if circumstantial evidence indicates that the launching State failed to require private operators to observe precautions that resulted in physical damage to third States, although the private operator had the technical means and time to mitigate the risk, and knowledge of the risks. In such situation, the launching State would have an obligation to compensate the third State that had suffered damage in outer space under the Liability Convention's terms.

4.2.4 The Liability Convention and Damage on Earth

The regime of the Liability Convention is different when damage occurs due to cyber interference with a space object that results in a collision with aircraft in flight or damage on the Earth's surface.

---

71 Black's Law Dictionary 559 (6th ed.1991).

72 *Id.*, at 716.

73 In *The Corfu Channel Case*, the International Court of Justice highlighted the importance of 'recourse of inferences of fact and circumstantial evidence': '[…] the fact of this exclusive […] control […] has a bearing upon the methods of proof available to establish the knowledge of that State as to such events. By reason of this exclusive control, the other State, the victim of a breach of international law, is often unable to furnish direct proof of the facts giving rise to responsibility. Such a State should be allowed a more liberal recourse of inferences of fact and circumstantial evidence. The indirect evidence is admitted in all systems of law and its use is recognized by international decisions. It must be regarded as of special weight when it is based on a series of facts linked together and leading logically to a single conclusion'. In *The Corfu Channel Case* British ships suffered damage from the explosion of mines in an international stretch within Albania's territorial sea. Albania failed to inform British ships about the danger and later denied having knowledge of the mines. *The Corfu Channel Case* (UK v. Albania) (Merits) 1949 I.C.J. Rep. 4 (Apr. 9), at 18.

The Liability Convention states in its Article 2: 'A launching State shall be absolutely liable to pay compensation for damages caused by its space object on the surface of the Earth or to aircraft in flight.' In such an event there is no need to prove fault on the part of the launching State. A State that suffers damage needs only to prove the existence of damage and a causal connection between the space object and the damage. Thus, the State with the legal link to the space object that caused the damage is absolutely liable to compensate.

The fact that cyber activity is the origin of a sequence of events that finally results in physical damage does not release the State from responsibility for the space object, even if the cyber activity was beyond the control of that State.[74]

4.2.5 Recovery of Damages

A State liable under the Liability Convention for damage in outer space, on the Earth or to an aircraft in flight, may in turn attempt to recover the compensation paid from the perpetrator of the cyber activity, if known. But as a cyber activity is not a space activity, Article VI of the Outer Space Treaty does not apply and the recovery cannot be directed against the State of the perpetrator. Under space law, the State of nationality of the perpetrators of an unauthorized cyber activity has no obligation to directly compensate for damages, so the responsible State of the space object may not recover financial compensation paid to a third States for physical damages and would also have no compensation for the loss of its operational space object. Remedies at national level in national courts may be possible by punishment of individuals or institutions, but full recovery of the financial damage appears improbable.

5. Proposals for Legal Regulation

Cyber interference with space objects opens a new dimension of threat and new vulnerabilities. The satellite service and the space object itself can be partially or totally lost. It seems only a matter of time until an individual, a group of individuals or a private or governmental institution manipulates the flight controls of a satellite to transform it into a 'weapon' with enough kinetic energy to cause damage in outer space, or on the surface of the Earth. In many instances the perpetrators may remain anonymous, and new technology to identify perpetrators will be in a continuous race with technology to hide them.

---

74 In the case of Cosmos 954, which contaminated a vast area in Canada, the USSR accepted responsibility but disclaimed liability, arguing that environmental damage was not included in the definition of 'damage' of the Liability Convention. There is plenty of literature about this incident. A clear and brief explanation on the legal aspects is provided by Lyall & Larsen, Space Law, *supra* note 22, at 117. The Russian researcher Terekhov was of the opinion that, at the end, the USSR paid part of the costs following an *extra gratia* settlement. Terekhov, *International Liability for Damage Caused by Space Objects with Nuclear Power Sources on Board*, Proceedings of the Colloquium on the Law of Outer Space (IISL, 1993).

Expensive state-of-the-art technology in ground stations can help to avert unauthorised cyber activities, but the yawning gap between the rapid development of computer technology on the ground and aging computer systems on board the satellites make the space element the more vulnerable part of the system. There is no possibility of upgrading the hardware of computer systems on board space objects from ground stations, and installation of new software sent from Earth to the computer devices in space cannot help if the outdated and obsolete computer hardware cannot support the software. At present, it is not possible to perform in-orbit servicing of space objects by upgrading them constantly with new computer systems. Although such servicing is in development, it is assessed that it will be both expensive and technologically challenging. Ground stations without a high level of protection and radio links remain possible gateways for malware to render space object useless, or to manipulate them in dangerous ways.

What is left to do? The following proposals should be considered in order to overcome the shortcomings of current space law in regard to imminent unauthorised cyber activities with a destructive effect on space systems.

5.1 Prohibition of Unauthorised Cyber Activities against Space Objects

Cyber activities performed against space systems which result in the loss of control or service or in its destruction should be treated like piracy in international sea law or like unlawful seizure in air law, and be prohibited. The Outer Space Treaty states in its Article VIII:

> A State Party to the Treaty on whose registry an object launched in outer space is carried shall retain jurisdiction and control over such object […] while in outer space or on a celestial body. Ownership of objects launched into outer space, including objects landed or constructed on a celestial body, and of their component parts, is not affected by their presence in outer space or on a celestial body or by their return to the Earth […].

The purpose of this Article is to grant permanent rights to the State that 'registers' a space object[75]. Jurisdiction and control are permanently vested in that State. The US scholar Carl Christol clarifies the terms 'jurisdiction and control' in the following manner:

[75] The *Convention on Registration of Objects Launched into Outer Space* (1975) (Registration Convention) addresses more specifically the 'registration' issue. In the definitions section of this treaty, 'launching State' is addressed in the same manner as in the Liability Convention: a State that launches a space object, procures its launch, from whose territory a space object is launched or from whose facility it is launched. Registration Convention, Article I (a), *supra* note 25. In addition, the Registration Convention also indicates that launching States shall register their space objects in a national register and provide information to the Secretary-General of the United Nations. Registration Convention, Articles II(1) and IV, *supra* note 25. By 2013, the Registration Convention has been ratified by 60 States. See UN Status of International Agreements relating to Activities in Outer Space, *supra* note 33.

> '[J]urisdiction and control' have very important and separate meanings. But both stem from national sovereignty. 'Jurisdiction' is the basis relied on by a country to pass laws in which it asserts the legal claim that it has exclusive legal authority. 'Control', on the other hand, is used to complete the concept of national sovereignty, e.g., full physical and exclusive authority [over the space object].[76]

The meaning of 'control' in the Outer Space Treaty reaches beyond material control over a space object. Even if the State has no technical capabilities to operate or manoeuvre a space object (e.g., due to malfunction, lack of fuel) it still keeps legal control, and such rights should be respected. In international air and sea law, ownership provisions on aircraft[77] and maritime vessels[78] are complemented by provisions that prohibit their unlawful seizure or piracy.

Although Article VIII of the Outer Space Treaty spells out States' rights over their space objects, an explicit internationally binding rule is needed that prohibits unauthorised seizure of space objects through cyber activities.

5.2 Duty to Notify the International Community of Cyber Activities against a Space Object

A rule should oblige launching States to immediately inform the international community when one of their space objects is subject to an unauthorised cyber activity, and about related potential dangers. States that have knowledge about the development of cyber activities against a space object should immediately inform the launching State. In such circumstances, the launching State should take all necessary measures to avert the effects of the cyber activity and, if it has no means to put a timely stop to such an

---

76 Carl Christol, personal communication with the author, 11 August 2007.

77 Article 17 of the *Convention on International Civil Aviation* of 1944 (Chicago Convention) indicates that '[a]ircraft have the nationality of the State in which they are registered.' *Convention on International Civil Aviation,* entered into force Apr. 4 1947, 8 U.S.T. 179, 15 U.N.T.S. 295. Unlawful seizure of aircraft is addressed in Article 1 of the *Convention for the Suppression of Unlawful Seizure of Aircraft* of 1970 (Hague Convention): 'Any person who on board an aircraft in flight (a) unlawfully, by force of threat thereof, or by other form of intimidation, seizes, or exercises control of, that aircraft, or attempts to perform any such act, or (b) is an accomplice of a person who performs or attempts to perform any such act commits an offence.' Article 2 indicates: 'Each Contracting State undertakes to make the offence punishable by severe penalties.' *Convention for the Suppression of Unlawful Seizure of Aircraft* of 1970, entered into force Oct. 14 1971, 860 U.N.S.T. 105.

78 Article 91 of the *United Nations Convention on the Law of the Sea* (UNCLOS) refers to nationality of ships, while Articles 100 to 107 address piracy of ships and aircraft. Article 104 indicates: 'A ship or aircraft may retain its nationality although it has become a pirate ship of aircraft. The retention or loss of nationality is determined by the law of the State from which nationality was derived.' *United Nations Convention on the Law of the Sea* (UNCLOS), 12 UST 794, 402 U.N.S.T. 71. Piracy is defined in Article 101 UNCLOS as '(a) any illegal acts of violence of detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State; (b) any act of voluntary participation in the operation or a ship or of an aircraft with the knowledge of facts making it a pirate ship or aircraft; (c) any act of incitement or of intentionally facilitating an act described in subparagraph (a) or (b).' *Id.*

event, should request international assistance. International rules on suitable procedures for such situations should be adopted.

5.3 International Responsibility and Liability of States that Authorise Cyber Activities against Space Objects of Other States without Consent

The obligations accepted by launching States through the Liability Convention should not be affected by cyber activities that have an effect similar to piracy in international sea law or unlawful seizure in air law.

It remains difficult to attribute cyber activities to individuals or institutions. Nevertheless, as was reported to the US Congress, '[a]ttribution of these threats remains problematic, but security researchers can increasingly group incidents into campaigns. Monitored over an extended period, these factors provide a more complete understanding of the actors responsible for intrusions.'[79] Traditionally, States are not responsible for the acts of persons or a group of persons not acting on behalf of the State,[80] but Article VI of the Outer Space Treaty introduced to public international law the exceptional innovation that States are accountable for the space activities of their non-governmental institutions. A rule should extend the responsibility and liability regime under space law if cyber forensics can undoubtedly and objectively pinpoint the State which supported or authorised the cyber activity against a space object. The launching and operating States of a space object that suffers damage due to the activity of another State should be entitled to compensation from the State that supported or authorised a cyber activity, or acted with negligence by not taking measures to stop such an act.

5.4 Application of Space Debris Mitigation Measures

The lack of financial and technical possibilities for refurbishing on-board computer hardware, so that it that can resist destructive cyber activities, puts a stronger onus on States to properly apply measures to minimise potential residual dangers of their national space objects before decommissioning.

---

79 2012 Annual Report to Congress of the U.S.-China Economic and Security Commission, 112th Congress, 2nd Session (Nov. 2012), Section II, China's Cyber Activities, at 153, http://www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf.

80 See International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, UN Doc. A/RES/56/83 (2001), annex, Article 11.

The IADC, a non-governmental organisation with membership drawn from the majority of space agencies,[81] published in 2002 the Space Debris Mitigation Guidelines,[82] which were endorsed in 2007 in a UN General Assembly Resolution[83] (UN Space Debris Mitigation Guidelines). The UN Space Debris Mitigation Guidelines recommend post-mission disposal measures like clearing valuable orbits by transferring space objects approaching their end of operations to areas of lower collision risk.[84] The UN Space Debris Mitigation Guidelines also address the dangers of energy stored in space objects and recommend 'passivating' them before terminating their service. This measure would not only diminish the potential of break-ups in outer space but also reduce the possibility that space objects that still have intact flight control systems and fuel remnants may be reactivated and misused or directed to cause damage. Evolving State practice has been noticed in regard to several of the UN Space Debris Mitigation Guidelines.[85]

5.5 Adopting International Rules Banning Damaging Cyber Activities against Space Systems

These proposed rules could be integrated into a legal instrument, or become part of amendments to the Outer Space Treaty and the Liability Convention. UN COPUOS is the proper forum for the negotiation of such proposals. Independently, and parallel to the work of COPUOS, a scientific and technical platform should be established to address this problem and produce draft guidelines aimed at averting unauthorised destructive cyber activities against space systems. This work could be taken up by a group of technical experts following the model of the IADC which has accomplished exemplary work by establishing the basis for State practice and *opinio iuris* in several of its recommendations on space debris mitigation. These have become the fabric for the creation of international customary norms which, once established, are legally binding

81 Founding members of the IADC in 1993 were the European Space Agency (ESA), the National Aeronautics and Space Administration (US), the Japanese Aerospace Exploration Agency and ROSAVIAKOSMOS (Russian Federation). Following members were Agenzia Spaziale Italiana (ASI-Italy), the British National Space Council (BNSC-UK), Centre National d'Etudes Spatiales (CNES-France), the Canadian National Space Agency, Deutsche Luft- und Raumfahrt Agentur (DLR-Germany), the Indian Space Research Organization and the National Space Agency of Ukraine (NSAU-Ukraine).

82 IADC Space Debris Mitigation Guidelines, *supra* note 46.

83 UN GA, 'International Cooperation on the Peaceful Uses of Outer Space', UN Doc. A/RES/62/217 (2008), § 27. Report of the Committee on the Peaceful Uses of Outer Space, UN GAOR, 62nd Sess., Supp. No. 20 at § 117-128, UN Doc. A/62/20 (2007). The UN Space Debris Mitigation Guidelines are included in this document's annex.

84 See 5.3.1. 'Geosynchronous region' and 5.3.2. 'Objects passing through the Low Earth Orbit Region', UN Space Debris Mitigation Guidelines. *Id.*

85 Martha Mejía-Kaiser, *Taking Garbage Outside: The Geostationary Orbit and Graveyard Orbits*, in IISL Proceedings on the Law of Outer Space (2006); Martha Mejía-Kaiser, *Informal Regulations and Practices in the Field of Space Debris Mitigation*, Air and Space Law 34, no. 1, 21-34 (2009); Nicholas Johnson, *The Disposal of Spacecraft and Launch Vehicle Stages in Low Earth Orbit,* Proceedings of the Advancement of Space Safety Conference (2007).

upon all members of the international community, even if they are not integrated into an international treaty.[86]

5.6 *Res Communis* of Outer Space as a Model for Cyberspace

The Outer Space Treaty adopted the *res communis* principle in its Article 2, which states that '[o]uter space, including the Moon and other celestial bodies, is not subject to national appropriation […]'.[87] Such principle mirrors the approach taken in international law to the high seas. Brownlie notes that 'States are bound to refrain from any acts which might adversely affect the use of the high seas […]' and continues '[i]t is generally accepted that outer space and celestial bodies have the same character.'[88] This may not be applicable directly to cyberspace, but the two share some characteristics.

Cyberspace has been artificially created by humans and requires infrastructure that is stationed in the territories of sovereign States. However, like outer space, cyberspace is a realm without boundaries. It serves the whole international community and, due to the increasing dependency of the world economy and critical safety functions, must be kept operational.[89] Many principles laid down in the Outer Space Treaty should also apply to cyberspace, for example:

- Its use shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development.[90]
- It shall be free for use by all States (and their nationals) without discrimination of any kind, on a basis of equality and in accordance with international law.[91]
- Its use shall be in accordance with international law, including the *Charter of the United Nations*, in the interest of maintaining international peace and security and promoting international cooperation and understanding.[92]

Consequently, States should not authorise or tolerate destructive cyber activities performed in their territories or by their nationals, but should enact legislation to prohibit the use of detrimental cyber activities, especially those that affect international foreign interests, and to establish mechanisms to punish such acts. In case of disputes due to destructive cyber activities, States should not retaliate with offensive cyber activities, but should use the available peaceful dispute settlement mechanisms.

86 Martha Mejía-Kaiser, *Informal Regulations, supra* note 85.

87 Outer Space Treaty, *supra* note 1, Article II.

88 Ian Brownlie, *supra* note 35, at xlii & 169.

89 Gary Brown & Owen Tullos present several cases where unauthorised cyber activities have forced institutions to deactivate computer systems from hours to almost a month. Gary Brown & Owen Tullos, *On the Spectrum of Cyberspace Operations*, in Small Wars Journal, (Dec. 12, 2012), http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.

90 Outer Space Treaty, *supra* note 1, Article I(1).

91 *Id.*, Article I(2).

92 *Id.*, Article III.

6. Conclusions

In recent years, although few cyber activities have been performed on space systems,[93] several destructive cyber activities have taken place in other areas at international level, causing different types of damage at different magnitudes.[94] Each evolutionary phase of cyber activities creates new vulnerabilities. Space objects are the most vulnerable element for the entrance of unauthorised cyber activities.

Space activities are ultra-hazardous activities that can affect any State.[95] Lyall and Larsen noted '[…] any damage [in outer space] is likely to occur swiftly and may often be catastrophic. Space activities are inherently dangerous so it is right that they should be properly supervised, and that liability should follow in the event of damage.'[96] Unauthorised cyber activities affecting space systems will confront the international community with new dangers. The present state of space law, in particular the Outer Space Treaty and the Liability Convention, has shortcomings that will unfairly impose responsibility and liability on launching States for damage caused by unauthorised cyber activities, even when supported or authorised by other States.

Damage resulting from cyber activities performed against space objects should be addressed at the State level, because only States have the legal and financial capacity to respond to such damage. State responsibility and liability, as it exists for space activities, should therefore be established for unauthorised cyber activities against space objects that lead to damage in outer space or on the Earth.

The drafters of the Outer Space Treaty and the following space treaties foresaw developments in the distant future and paved the way for international cooperation and the peaceful use of a common domain. Such pioneering work can serve as a model for the creation of 'international cyber law'.

---

93 Besides the cases cited in section 2 of this chapter, the international press reported that in 2007 unauthorized access was gained to the remote sensing US satellite Landsat-7, which gathers remote sensing data for civilian uses. It has not been disclosed whether data was retrieved or the perpetrator was just assessing the hacking abilities. John Leyden, *supra* note 7.

94 Gary Brown & Owen Tullos make an account of important cyber activities, some of them with destructive effects. Brown & Tullos, *supra* note 89.

95 Manfred Lachs, The Law of Outer Space, An Experience in Contemporary Law-Making, xiii, 113-124 (1972, *reprinted in* 2010).

96 Lyall & Larsen, Space Law, *supra* note 22, at 66.

Joel P. Trachtman

International Economic Law in the Cyber Arena

1. Introduction

Cyber security activities, both defensive and offensive, may raise issues under international economic law. There are two main questions. Firstly, what types of possible cyber operations might violate particular provisions of international economic law, including trade, investment, and intellectual property law? And secondly, to what extent are the rules of international economic law qualified by national security exceptions that may allow defensive or offensive cyber operations that would otherwise violate the rules? Since most international economic law is in the form of treaty, the first question is largely one of treaty review and analysis. Since most potentially relevant exceptions are explicitly incorporated in treaty, the second question also involves analysis of national security or other potentially applicable exceptions. There is also the possibility that the customary international law necessity exception may be relevant in connection with international economic law obligations, either by way of interpretation or by way of application, or both.

This chapter first provides a brief taxonomy of cyber operations that may raise international economic law issues. It then presents subject matter for review under potentially applicable international economic law, including trade, investment, and intellectual property law. This chapter also evaluates the possible application of security exceptions to allow cyber operations that might otherwise violate international economic law. This brief chapter cannot review the complete field of international economic law treaties, but selects some important and notable examples for analysis in a way that will inform the analysis of other treaties.

2. A Taxonomy of Cyber Operations that May Raise International Economic Law Issues

It is useful to begin by describing the types of cyber operations with which this chapter is concerned. The focus is on offensive and defensive cyber operations: cyber attack and cyber defence.

'By "cyberattack," we usually mean a software program transmitted over digital networks and installed covertly on a target machine to disrupt data or services or destroy machinery. The stuxnet virus is a good example of this type of cyberattack. Similar techniques can also be used for espionage, substituting the exfiltration of data

for damage or disruption.'[1] Cyber attack is less diverse than cyber defence, and there is only a limited body of international economic law that may be applicable. Most international economic law was established for a purpose quite separate from deterring cyber attack.

In addition to transmission over digital networks, it is possible that cyber attack can take place through the use of software delivered physically. Software can be delivered by embedding it in equipment that is subsequently delivered, or by inserting it in equipment that is already *in situ*. The only body of international economic law that may possibly restrict cyber attack is intellectual property law, and even here the argument is rather weak.

Cyber defence includes measures designed to repel cyber attack, and raises a broader range of international economic law rules; for our purposes, defensive measures in the form of counter-attack using cyber operations can be covered under 'cyber attack.' It is important that cyber attack can be transmitted across borders either through networks, through equipment, or by human activity accessing networks or equipment *in situ*. Cyber attack can focus on government-owned security assets, other government-owned assets such as transportation, power, or communications infrastructure, or privately-owned critical infrastructure assets.

Defensive measures raise international economic law issues when they block or restrict these types of transmission. Generally speaking, these measures only raise international legal issues when they are carried out by governments, or when they are carried out by private persons where the government has an international legal duty to prevent the private person from taking the action at issue.

In economic law terms, we may speak of trade in services through electronic transmission; trade in goods; trade in services through cross-border movement of service providers or through commercial presence; and foreign investment relating either to services, in which case it is the same as commercial presence, or to production or preparation of goods. The following table aligns means of delivery with possibly applicable rules of international economic law.

[1] James A. Lewis, Conflict and Negotiation in Cyberspace 11 (2013), available at https://csis.org/publication/conflict-and-negotiation-cyberspace.

Potentially Applicable Bodies of Law					
Means of Delivery	**Trade in Goods Law**	**Government Procurement Law**	**Trade in Services Law**	**Foreign Investment Law**	**Intellectual Property Law**
Network	*Inapplicable*	*Applicable*	*Applicable*	*Inapplicable*	*Possibly applicable*
Movement of equipment	*Applicable*	*Applicable*	*Inapplicable*	*Inapplicable*	*Inapplicable*
Human activity *in situ*	*Inapplicable*	*Applicable*	*Applicable*	*Applicable*	*Possibly applicable*

For purposes of illustration, I provide below some examples of measures that States may take in order to defend against cyber attacks:

- Impose standards for cyber security with respect to government procurement of goods or services for military use.
- Impose standards for cyber security with respect to government procurement of goods or services in connection with other governmental operations.
- Impose standards for private sector purchases of goods or services involved in security operations.
- Impose standards for private sector purchases of goods or services involved in critical infrastructure provision.
- The standards listed above may be applied generally to all government and private operations, or only to those where transactions with specified foreign countries are contemplated. Certain foreign countries may develop safeguards that may be recognized as satisfactory as host country standards.
- Impose restrictions on foreign investment in security or critical infrastructure operations. These restrictions may either prohibit or set standards for all foreign investment, or focus on particular countries.

Below, I discuss the international economic law that is potentially applicable to these offensive and defensive cyber operations.

3. WTO Law

As of March 2013, the World Trade Organization (WTO) had 159 Member States. The WTO treaty contains requirements for States to reduce barriers to access to their markets for goods (the *General Agreement on Tariffs and Trade* or GATT) and, to a limited extent, services (the *General Agreement on Trade in Services* or GATS). The obligations under GATT with respect to product standards and technical regulations

are elaborated further in the *Agreement on Technical Barriers to Trade* (TBT). The WTO also includes the *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS). Finally, the WTO includes a plurilateral *Agreement on Government Procurement* (GPA), amended as of 30 March 2012, to which 14 members, plus the 28 European Union (EU) members, adhere.[2]

This section will examine the WTO law restrictions contained in the GATT, TBT, GATS, and GPA. The subsequent section, addressing intellectual property, will discuss the TRIPS. I do not separately consider regional or plurilateral integration agreements such as the *North American Free Trade Agreement* or the European Union. These agreements (other than the European Union, which is *sui generis*) will often have similar structures to the WTO law discussed here, and sometimes even incorporate by reference provisions of WTO law.

Nothing in the GATT, TBT, GATS, or GPA imposes any prohibitions or requirements that would limit cyber attack as defined above. They focus more on restraining national protectionism against *imports* than on the safety or other qualities of *exports*. So, the discussion below focuses on defensive cyber operations. In particular, I focus on limitations on imports of goods or services from other WTO members. Treaty-based international economic law, such as the WTO, provides no rights to non-members.

It is not certain whether software would be treated as a good or as a service under WTO law.[3] Different States take different positions on this issue, and the treatment depends in part on whether the software is incorporated into a physical medium or piece of equipment.

In the following subsections, I discuss WTO law rules that discipline national barriers to trade in goods or services, or that discipline government procurement for countries party to the GPA. Subsequently, I discuss the security exceptions and general exceptions contained in each of these agreements, which might apply to relax these disciplines.

3.1 Trade in Goods

Nothing in GATT or the TBT would generally prevent an importing State from setting regulatory standards consistent with cyber security with respect to imported software. However, under the GATT, States commit to provide national treatment and most-

2 While the amendment has not entered into force at the time of writing, I focus on the language of the amendment because it is highly likely to be the operative law in the future. The Protocol will enter into force for those Parties to the 1994 GPA that have deposited their respective instruments of acceptance of this Protocol, on the 30th day following such deposit by two thirds of the Parties to the 1994 GPA. The parties to the GPA are Armenia, Canada, the European Union (with respect to its 27 Member States), Hong Kong-China, Iceland, Israel, Japan, Korea, Liechtenstein, the Netherlands (with respect to Aruba), Norway, Singapore, Switzerland, Chinese Taipei, and the United States.

3 For an analysis, *see* Althaf Marsoof, A Case for *Sui Generis* Treatment of Software Under the WTO Regime, *20 Int'l J. L. & Info. Tech*. 291 (2012).

favoured nation (MFN) non-discriminatory treatment to foreign goods in connection with domestic regulation. Under the TBT Agreement, States additionally commit not to impose technical regulations that are more trade restrictive than necessary.

Let us begin with the GATT. Assume that a State imposes cyber security based technical regulations on network equipment to be used in the national internet or other telecommunications grid. So long as these technical regulations do not discriminate between like products from foreign countries and domestically-produced products, or between like products from different foreign countries, they are acceptable under GATT. It is possible for national technical regulations of this type to be applied so as to afford protection from competition to domestic producers, or to prefer producers from a particular foreign country. However, provided that the result of the technical regulation is not excessively to advantage one national group of producers, it is unlikely that a successful challenge could be mounted based on the national treatment or MFN rules.

It is an interesting question whether States will continue to be able to design national regulation of imported products so as to ensure cyber security. Such national regulation might require telecommunications or data processing products to be designed so as to ensure that they are sufficiently resilient to cyber attack. Or it might require these products to be certified by a trustworthy person as free of certain vulnerabilities or Trojan horse-type code. It may be that in order to ensure cyber security, States would have to regulate not only the product itself, but the process by which the product is produced.[4] It may even be that States would determine that only goods that are produced in States with similar political systems or with sufficient regulatory structures can be trustworthy.

It is not clear under the WTO rules of national treatment and MFN that States would be permitted to condition access to their markets on compliance with a specification of the way in which goods are produced, the way in which the production of goods is regulated in the State of production, or the politics of the State of production. The so-called 'product-process distinction' or 'product and production method distinction' (PPM) is still a contentious issue. However, even if these types of conditions may be found to violate the national treatment or MFN requirements, they might be permitted under the exceptions of Articles XX or XXI of GATT, described below. Interestingly, the TBT Agreement also includes obligations of national treatment and MFN treatment, but lacks exceptions along the lines of Articles XX or XXI.[5] The scope of its national

4 See Theodore Moran, Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers, *Peterson Institute Policy Brief* [online] 13-11, dated May 2013, available at http://www.iie.com/publications/interstitial.cfm?ResearchID=2390.

5 Article 10.8.3 of the WTO *Agreement on Technical Barriers to Trade* (the 'TBT Agreement') contains a very narrow security exception dealing only with the disclosure of information. See the discussion below.

treatment requirement has recently been interpreted narrowly in order to avoid invalidating a broader scope of national standards than the GATT.[6]

If a State were to structure its standards so as to apply variably to imports of goods or services from different WTO members, this differentiation could raise issues under the MFN principle of Article I of GATT or Article II of GATS. However, if the differentiation is justified by a good faith (i.e., non-protectionist) cyber security rationale, it would be likely to be defensible under these MFN rules, or under the general exceptions discussed below.

In addition, under the TBT Agreement, national technical regulations are not permitted to be 'more trade-restrictive than necessary to fulfil a legitimate objective, taking account of the risks non-fulfilment would create.' National security requirements are explicitly included as 'legitimate objectives.' This necessity or proportionality test might be violated where there is a less trade-restrictive alternative means available to achieve the legitimate objective. However, WTO panels and the WTO Appellate Body, which is in effect the court of final appeal at the WTO, have been rather deferential to national decision-making under this test.[7]

Furthermore, Article 2(4) of the TBT Agreement provides as follows:

> Where technical regulations are required and relevant international standards exist or their completion is imminent, Members shall use them, or the relevant parts of them, as a basis for their technical regulations except when such international standards or relevant parts would be an ineffective or inappropriate means for the fulfilment of the legitimate objectives pursued, for instance because of fundamental climatic or geographical factors or fundamental technological problems.

Thus, international standards such as the network security provisions of ISO/IEC 27001,[8] to the extent that they constitute a 'relevant international standard' in relation to a proposed or existing national measure, are required to be used as a basis for the national measure, except as specified in Article 2(4). This imposes some limitation on the flexibility available to States to impose restrictions on importation of goods for cyber security purposes. However, the limitation would not seem to restrict the ability of a State to set a higher standard in order to achieve its nationally-determined 'appropriate level of protection.'

---

6 WTO, 2012, *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, WT/DS406/AB/R, adopted 24 April 2012, at paras. 96-102.

7 *See* WTO, 2007, *Appellate Body Report, Brazil – Measures Affecting Imports of Retreaded Tyres*, WT/DS332/AB/R, adopted 17 December 2007 (addressing a similar test under Article XX of GATT).

8 ISO/IEC 27033 Information technology – Security techniques – Network security (parts 1-3 published, parts 4-6 DRAFT), available at http://www.iso27001security.com/html/27033.html.

3.2 Trade in Services

In order to maintain cyber security, States may decide to regulate the provision of telecommunications, data processing, or other services. GATS is in part a 'positive list' agreement, meaning that some of its most significant disciplines only apply to the extent that a State has listed on its schedule of commitments the relevant service sector, in the relevant mode of international trade in services, such as 'cross-border provision' or 'commercial presence,' and has not specified an applicable exception in its schedule of commitments.

The disciplines that are dependent on scheduling are 'national treatment,' which is similar to the rule of national treatment non-discrimination in the GATT, and 'market access,' which is specifically defined to prohibit several specific types of quantitative or other similar restrictions on trade in services. For purposes of analysis, I assume that a State has commitments in these areas. All obligations discussed below are subject to security exceptions under Article XIV *bis* of GATS, addressed below.

The national treatment obligation under Article XVII of GATS requires each member to 'accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers.' Therefore, it would be required for cyber security regulation to be applied in an even-handed way to foreign services and service suppliers, and in relation to domestic services and service suppliers. If foreign services or service suppliers, as a class, presented enhanced cyber security risks, it is not necessarily a violation of national treatment to treat them differently in a way that is responsive to the enhanced risk.

The market access obligation under Article XVI of GATS, while expressly limiting the ability of States to impose quantitative and certain other narrowly specified types of restrictions, has been interpreted by the WTO Appellate Body to apply to restrictions that might ordinarily be understood as *qualitative*. In the *US-Gambling* case, the Appellate Body found that restrictions on cross-border internet gambling services violated this restriction.[9] So it is possible that cyber security restrictions applied to services might similarly be found to violate this restriction.

Article II of GATS contains an MFN obligation which applies regardless of scheduling. This obligation may make it illegal to treat service providers of allied or trusted countries differently from those of other States.

Finally, Article VI of GATS provides a complex discipline on domestic regulation of imported services. In essence, WTO members are not permitted to apply technical standards that nullify or impair specific commitments in a manner that is more

9 WTO, 2005, *Appellate Body Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, adopted 20 April 2005.

burdensome than necessary to ensure the quality of the service and could not reasonably have been expected at the time the specific commitments were made.

3.3 Government Procurement

Importantly, as noted above, the GPA is a plurilateral trade agreement, and such agreements do not create either obligations or rights for the members that have not accepted them. The GPA applies to procurement for governmental purposes of both goods and services, and it is a positive list agreement, meaning that its obligations are dependent on scheduling of the covered products, services, and government entities.

The GPA also includes in Article IV obligations of national treatment and MFN treatment. On this basis, a member of the GPA cannot exclude suppliers that are nationals of other GPA members from tendering, or treat them or their products or services less favourably than they treat local suppliers or suppliers from third GPA members. Therefore, it may be illegal to exclude suppliers purely on the basis of nationality.

In addition, a procuring entity is required under Article VIII to limit conditions for participation to those that are essential to ensure that the supplier has the legal and financial capacities and the commercial and technical abilities to undertake the relevant procurement. This obligation may make it difficult to impose cyber security conditions for participation.

States subject to these obligations would want to be sure to include cyber security parameters as part of the technical requirements relating to their procurement. Finally, Article X of the GPA states that 'a procuring entity shall not prepare, adopt or apply any technical specification or prescribe a conformity assessment procedure with the purpose or the effect of creating unnecessary obstacles to international trade.' Under this requirement, technical specifications and conformity assessment intended to achieve cyber security goals must be the least-restrictive alternative to achieve the goal.

3.4 Security Exceptions

Article XXI of GATT, Article XIV *bis* of GATS, and Article III of the GPA provide security exceptions. Interestingly, these exceptions have different scopes of application. To the extent that these exceptions may apply, they would excuse measures that violate the provisions discussed above. Of course, the exceptions only become relevant if there is a violation.

GATT. Article XXI of GATT provides that nothing in the GATT 'shall be construed [...] to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests [...]; (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as

is carried on directly or indirectly for the purpose of supplying a military establishment; or (iii) taken in time of war or other emergency in international relations [...].'

GATS. Article XIV *bis* of GATS provides in relevant part that nothing in the GATS 'shall be construed [...] to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests: (i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment; [...] [or] (iii) taken in time of war or other emergency in international relations [...].'

GPA. Article III of the GPA provides that '[n]othing in this Agreement shall be construed to prevent any party from taking any action [...] that it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes.'

Curiously, while the TBT Agreement contains a provision providing that members shall not be required to furnish any information, the disclosure of which they consider contrary to their national security interests, it does not address the security issues addressed in the language of the other agreements excerpted above.

I will review the potential applicability of these exceptions in turn.

There has been much heated discussion, but little authoritative illumination, of the scope of the Article XXI exception in GATT. Often, diplomats, journalists, and some scholars describe the GATT Article XXI exception as 'self-judging,'[10] meaning that each State decides for itself whether to use the exception, and the rationale for its use is not subject to dispute settlement. However, this perspective has not been confirmed in dispute settlement, and the language of Article XXI suggests a more nuanced approach. This approach recognizes that the existence of the enumerated conditions is not self-judging; rather, what is self-judging is whether the national measure is *necessary* for the protection of the State's essential security interests in response to the existence of the relevant enumerated condition.[11] The better reading is that the necessity is subjective, but the existence of the war or other emergency is objective.

One might analyze the central aspect of the Article XXI security exception as comprising three components. In order to qualify for the exception, the national measure must be (a) necessary, (b) for the protection of the acting State's essential security interests, and (c) taken in time of war or other emergency in international relations. Now, what do we do with the subjective language: 'which it considers?' It may be read to modify any or all of (a), (b), or (c), although there is no doubt that it modifies (a), and for many

10 See, e.g., Roger P. Alford, The Self-Judging WTO Security Exception, *3 Utah L. Rev.* 697 (2011).

11 See Dapo Akande & Sope Williams, International Adjudication on National Security Issues: What Role for the WTO?, *43 Va. J. Int'l L.* 365, 399-400 (2003).

commentators there is little doubt about (b). Thus, the major interpretive question in connection with the degree to which Article XXI is self-judging is whether the language 'which it considers' relates only to whether the measure is 'necessary for the protection of its essential security interests' or whether it also relates to the enumerated conditions. Given the grammatical structure of Article XXI, it is not possible to adduce from the plain language itself which of these conditions is included in the phrase 'which it considers' – and thus which is self-judging. There is no dominant interpretive rule that can definitively answer this question, but a focus on the ordinary meaning of the language would tend to separate the phrase 'which it considers necessary for the protection of its essential security interests' from the enumerated conditions.

In particular, assuming that the enumerated conditions are not self-judging, there is an important question whether a 'war or other emergency in international relations' exists. 'War' would presumably include both declared and undeclared wars, and even sustained 'wars' on terrorism.[12] In modern times, it would not appear to be limited to interstate warfare, and indeed, in the context of Article XX of GATT, the WTO Appellate Body has taken an evolutionary approach to interpreting the definition of 'exhaustible natural resources,' which occupies a similar grammatical position.[13] The definition of 'other emergency in international relations' seems more difficult to interpret, but it would not seem to include ordinary course protections against cyber security vulnerability. One definition of 'emergency' is a 'serious, unexpected, and often dangerous situation requiring immediate action.'[14] The extent to which ordinary precautions against cyber attack may under certain circumstances fall within this definition is uncertain.

Given this uncertainty, and the fact that there has been no authoritative interpretation, it is worthwhile briefly to review how Article XXI has been used by States.

In the 1940s, under the Marshall Plan, the United States (US) established export controls on certain products that were in short supply or that had military significance. These products were routinely licensed for export to Western Europe, but were restricted for export to Eastern Europe. Czechoslovakia challenged the US administration of its export controls as a violation of the MFN rule of non-discrimination. However, in the GATT Council, Czechoslovakia's proposal for the establishment of a working party to examine

12 On the other hand, in the proposed draft *Multilateral Agreement on Investment*, the security exception was proposed to refer to measures 'taken in time of war, or armed conflict, or other emergency in international relations.' This would suggest that at least some do not intend 'war' to include all armed conflict. Organization for Economic Cooperation and Development, Negotiating Group on the Multilateral Agreement on Investment, *The Multilateral Agreement on Investment*, Draft Consolidated Text, DAFFE/MAI(98)7/REV1, 22 April 1998, available at www1.oecd.org/daf/mai/pdf/ng/ng987r1e.pdf.

13 WTO, 1998, *Report of the Appellate Body, United States – Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, adopted 12 October 1998, para. 130.

14 http://oxforddictionaries.com/us/definition/american_english/emergency.

its complaint failed by a vote of 17 against, 3 abstained, and 1 (Czechoslovakia) for.[15] This is by no means binding or even strongly suggestive of whether indeed any part of Article XXI is 'self-judging,' although it may be useful in interpretation of subsequent practice. It does suggest that States have generally sought to avoid litigation over the security exception.

In connection with the Falklands War between the United Kingdom and Argentina, the European Community imposed a trade embargo against Argentina in 1982. Argentina complained in GATT, but no GATT dispute resolution panel was established because there was no consensus to do so. During the pre-WTO period, consensus was required to take dispute resolution (and other) action under GATT practice.

In 1985 the US imposed an embargo on Nicaragua, and Nicaragua complained to GATT. The US resisted establishment of a GATT panel until the mandate to the panel included the limitation 'that the Panel could not examine or judge the validity of or motivation for the invocation of Article XXI:(b)(3) by the United States in this matter.'[16] The panel raised concerns about this approach:

> If it were accepted that the interpretation of Article XXI was reserved entirely to the contracting party invoking it, how could the CONTRACTING PARTIES ensure that this general exception to all obligations under the General Agreement is not invoked excessively or for purposes other than those set out in this provision? If the CONTRACTING PARTIES give a panel the task of examining a case involving an Article XXI invocation without authorizing it to examine the justification of that invocation, do they limit the adversely affected contracting party's right to have its complaint investigated in accordance with Article XXIII:2?[17]

The US blocked adoption of the panel report, and so the panel report has no precedential or other legal effect.

In two subsequent situations, relating to a European Community embargo on Yugoslavia in 1991 and a US secondary boycott against Cuba in 1996, panels were established under new procedures that did not require consensus. However, due to political solutions to each of these situations, the panel proceedings were not continued to conclusion.[18]

Thus, it is uncertain how far the self-judging nature of the Article XXI exception extends, but it seems reasonable to conclude that, assuming there is a war or other

---

15 GATT Council, 1949, *Summary Record of the Twenty-Second Meeting,* at 9, CP.3/SR.22 (8 June 1949), available at http://www.wto.org/gatt_docs/English/SULPDF/90060100.pdf.

16 GATT Council, 1985, *Minutes of Meeting Held in the Centre William Rappard on Oct. 10, 1985*, at 6, C/M/192 (24 Oct. 1985), available at http://www.wto.org/gatt_docs/English/SULPDF/91170093.pdf.

17 GATT, 1986, *Panel Report, United States – Trade Measures Affecting Nicaragua*, paras. 5.1–5.17, L/6053 (13 October 1986), available at http://www.wto.org/gatt_docs/English/SULPDF/91240197.pdf.

18 For a more specific account, *see* Alford, *op cit,* at 716-721.

emergency in international relations within the language of Article XXI, at least the degree to which a measure is necessary for the protection of the acting State's essential security interests is self-judging.

Article XIV *bis* of GATS contains identical relevant language, and can be expected to raise the same interpretive issues as Article XXI of GATT.

By contrast, the security exception contained in Article III of the GPA is remarkably limited. First, we have a similar interpretive question to that addressed with respect to Article XXI – to what part of Article III of the GPA does 'that it considers necessary' refer? However, the scope of action is not triggered by the existence, in relevant part, of war or other emergency in international relations. Instead, it is triggered by the 'procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes.' It is difficult to see how this covers procurement of civilian transportation or telecommunications infrastructure goods, or even nuclear power-plant control equipment. It is possible that this procurement could be understood as 'indispensable for national defence' in some circumstances, but that would often be an extension of what is ordinarily considered indispensable to national security. It is not the procurement itself that is indispensable, but the characteristics of the goods or services procured. For example, is procurement of non-military telecommunications equipment or railway software indispensable for national defence? So, first, it is difficult to understand Article III of the GPA as completely self-judging; and second, the trigger events seem more limited than those contained in Article XXI of GATS.

Indeed, while the public procurement covered by the GPA presents a major issue in terms of cyber security threats to or through public services or other public infrastructure, it seems to provide the narrowest exception.

To sum up on the role of the security exception in the WTO system, we must first say that there is some uncertainty regarding the justiciability and scope of the self-judging character of the security exceptions. With respect to GATS, we would have to examine individual countries' schedules of commitments in order to determine whether they have taken additional security exceptions within these schedules. The TBT Agreement does not contain a relevant security exception, and so in order to have a security exception with respect to obligations contained in the TBT Agreement, it would be necessary to argue that the GATT security exception somehow applies within this other agreement, despite the fact that Article XXI of GATT says that 'nothing in *this* agreement shall be construed to prevent [...].'[19] With respect to government procurement, we have a

[19] No WTO tribunal has examined whether the Article XXI exception would be available to defend against claims under the TBT Agreement. However, in the similar context of the Article XX general exceptions discussed below, the Appellate Body has declined to apply Article XX as an exception with respect to obligations under the TBT Agreement. Appellate Body Report, 2012, *United States – Measures Affecting the Production and Sale of Clove Cigarettes*, WT/DS406/AB/R, adopted 24 April 2012, at paras. 96-102. However, it has interpreted

security exception of narrower scope, which, for example, would not appear to cover cyber security based restrictions in public procurement of network equipment or railway controls if they were designed in a way that violated another provision of the GPS Agreement.

3.5 General Exceptions

In a pattern similar to that observed with respect to the security exception, each of the GATT, GATS, and GPA Agreements contains a general exception that may be applicable to cyber security defence operations. The TBT Agreement contains no explicit general exception. Article XX of GATT has been the basis for significant litigation in the WTO, and there has also been some litigation over the exceptional provision of GATS, Article XIV. The language of these exceptions is quite similar, and can be expected to be interpreted similarly. In this subsection, I will focus on Article XX of GATT.

Article XX of GATT provides in relevant part as follows:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any contracting party of measures:
>
> [...] (b) necessary to protect human, animal or plant life or health [...].

Focus first on clause (b). Could restrictions on imports of goods (or services under the similar language of Article XIV of GATS) be necessary to protect human life or health? This provision is definitely not self-judging, but it is easy to see many cyber security defensive measures as 'necessary to protect human life.' In clause (a) of the similar provision of GATS, there is a reference to measures 'necessary to protect public order.' Many cyber security defensive measures may come under this clause also. The word 'necessary' in this context has been interpreted extensively. In some cases, the Appellate Body has explicitly interpreted this provision as requiring a balancing approach. In others, it has appeared to back away from a full balancing approach by permitting the member to choose its 'level of protection' and then validating the national measure if this level cannot be reached through a less trade-restrictive means.

The Appellate Body most notably formulated and applied a judicial balancing approach in a case involving a requirement of the Republic of Korea that retailers make a choice

the TBT Agreement obligations narrowly in order to reflect the values of the Article XX exception. In light of the Appellate Body's decision in *China – Raw Materials*, members may only expect to rely directly on GATT Article XX exceptions when the provisions of another covered agreement explicitly refer to the GATT. See Appellate Body Report, 2012, *China – Measures Related to the Exportation of Various Raw Materials*, WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R, adopted 30 January 2012, at paras. 303-306.

of only selling Korean or foreign beef.[20] In that case, Korea argued that its requirement was necessary to facilitate monitoring of the labelling of the origin of beef sold in Korea, and to ensure compliance with regulations against deceptive marketing. The Appellate Body applied a judicial balancing test involving three variables to determine whether the Korean measure was 'necessary' to secure compliance with Korea's anti-fraud regulations under its *Unfair Competition Act*, within the meaning of Article XX(d) of the GATT. The Appellate Body concluded:

> In sum, determination of whether a measure, which is not 'indispensable', may nevertheless be 'necessary' within the contemplation of Article XX(d), involves in every case a process of *weighing and balancing* a series of factors which prominently include the contribution made by the compliance measure to the enforcement of the law or regulation at issue, the importance of the common interests or values protected by that law or regulation, and the accompanying impact of the law or regulation on imports or exports.[21]

In subsequent cases, the Appellate Body, although it has consistently referred to the *Korea-Beef* balancing test, has avoided requiring panels to engage in explicit judicial balancing. It has applied the least trade-restrictive alternative test after finding that the purpose of the regulatory measure was to reduce a given risk as much as possible. For example, in *EC-Asbestos*, the Appellate Body determined that France's chosen level of protection was 'a "halt" to the spread of *asbestos*-related health risks.'[22] It found that the less trade-restrictive alternative proposed by Canada of 'controlled use' of asbestos would not contribute to the realization of this goal to the same extent as would a 'prohibition.'[23]

In *US-Gambling*, a GATS Article XIV case, the Appellate Body confirmed that a '"reasonably available" alternative measure must be a measure that would preserve for the responding Member its right to achieve its desired level of protection with respect to the objective pursued.'[24] Likewise, in *Brazil-Tyres*, the Appellate Body upheld the Panel's finding that 'Brazil's chosen level of protection is the reduction of the risks of waste tyre accumulation to the maximum extent possible,' and found that other measures could not contribute to the achievement of this objective in an equivalent manner.[25]

---

20 See WTO Appellate Body, 2005, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef* WT/DS161/AB/R & WT/DS169/AB/R, adopted 11 December 2000. See also WTO Appellate Body, 2005, *Dominican Republic – Measures Affecting the Importation and Internal Sale of Cigarettes* WT/DS302/AB/R, adopted 25 April 2005, at para. 70 (affirming the 'weighing and balancing' of these factors).

21 *See ibid*. at para. 164 (emphasis added).

22 Appellate Body Report, *EC—Asbestos*, WT/DS135/AB/R, 1 June 2001, at para. 168.

23 *Ibid*., at para. 174. *See* Gregory Shaffer & Joel Trachtman, Interpretation and Institutional Choice at the WTO, *52 Va. J. Int'l L* 103 (2011).

24 Appellate Body Report, 2005, *US-Gambling*, *op. cit.* at para. 308.

25 Appellate Body Report, *Brazil – Measures Affecting Imports of Retreaded Tyres*, WT/DS332/AB/R, adopted 17 December 2007, at paras. 144 and 156. Chad P. Bown & Joel P. Trachtman, Brazil – Measures Affecting

The general exception contained in Article III:2 of the GPA essentially tracks the provisions of Article XX of GATT discussed above. Therefore, for procurement covered by the GPA, States may derogate from their GPA obligations in order to effect measures necessary to protect human life or health, etc. In addition, the GPA seems to permit procuring States to establish specifications for goods or services, conditions for participation, or bidder qualification requirements that may relate to cyber security concerns. As mentioned above, with respect to specifications, Article X:1 provides that 'a procuring entity shall not prepare, adopt or apply any technical specification or prescribe any conformity assessment procedure with the purpose or the effect of creating unnecessary obstacles to international trade.' So, a necessity test, likely to be similar to that applied under Article XX of GATT, would apply to cyber security based technical specifications.

4. TRIPS and Multilateral Intellectual Property Law

Generally, international intellectual property law is intended to protect foreign-owned intellectual property in a host State. It does so by establishing certain obligations of States to protect intellectual property rights. For example, the main thrust of the WTO TRIPS Agreement is to establish substantive and enforcement standards for protection of intellectual property that are required to be implemented by Member States.

Article 10(1) of TRIPS provides that 'computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).' Article 9 of TRIPS states that 'members shall comply with Articles 1 through 21 of the Berne Convention (1971) and the Appendix thereto.' Article 12 of the *Berne Convention* provides that 'authors of literary or artistic works shall enjoy the exclusive right of authorizing adaptations, arrangements and other alterations of their works.'

This suggests that the authors of computer programs have the exclusive right of authorising alterations of their programs. Assume that State A hacks into the air traffic control system of State B by modifying its software. Is this an alteration of software that violates Article 12 of the *Berne Convention*, and therefore the TRIPS? If so, it would be subject to mandatory dispute settlement under the WTO *Dispute Settlement Understanding*, and possible multilaterally-authorised countermeasures by way of authorised suspension of concessions or other obligations by State B. If these obligations apply to the actions of States, they may restrict alteration of programs that are protected by copyright as part of a cyber operation, whether offensive or defensive.

There are three main questions that must be asked regarding the application of Article 12 to such cyber operations:

1. Do these obligations apply to State offensive cyber operations, such as hacking?

Imports of Retreaded Tyres: A Balancing Act, *8 (Special Issue 1) World Trade Review* 85 (2009).

The general approach of TRIPS seems to be to require protection of intellectual property from infringement both by private and public actors.

2. What is the territorial scope of application of Member States' TRIPS and *Berne Convention* obligations? The general approach of TRIPS is to regulate the intellectual property protection provided by WTO members within their own territory to intellectual property owned by nationals of other WTO members.[26] However, this principle is not made explicit, although it is arguable that it is implicit in the structure of the TRIPS and of the *Berne Convention*. On the other hand, Article 5(1) of the *Berne Convention*, which is incorporated into TRIPS, provides as follows:

   > Authors shall enjoy, in respect of works for which they are protected under this Convention, in countries of the Union other than the country of origin, the rights which their respective laws do now or may hereafter grant to their nationals, as well as the rights specially granted by this Convention.

   This national treatment provision could be interpreted as requiring Country A to protect the Article 12 (*Berne Convention*) rights of Country B nationals, within Country A. The key to applicability is protected works, not the territory in which those works are used. This is at least a plausible interpretation of Article 5(1), despite the reference to 'in countries of the Union,' because Article 5(1) can be understood as a grant of protection 'in countries of the Union,' separately from the place of use.

   Be that as it may, we must also ask where cyber operations are carried out. If a hacker physically located in Country A hacks software in Country B, where does the unauthorised alteration under Article 12 take place? The answer to this question is not obvious, and the most appealing answer may be that it takes place in both places: the hacker modifies the code in Country A, and then also modifies the code as it exists on a computer in Country B. So, if the hacker is physically located in Country A, the unauthorised alteration takes place in Country A. This is a factual and technical question, as well as a question of interpretation of the law.

3. Will the hacking be sufficiently attributable to constitute a 'measure' of Country A giving rise to responsibility of Country A under WTO law? This is a factual and technical question.

Cyber operations that merely engage in surveillance would not appear to raise issues under TRIPS, but defensive cyber operations that modify software may raise the same issues as those discussed above.

---

26 *See* David P. Fidler, Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage, *Arms Control Law Blog*, 11 February 2013, available at http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/.

It is uncertain whether patent protection is also available for software under TRIPS. However, the patent provisions of TRIPS do not provide any rules against modification, and so would not limit cyber activities that involve hacking.

The structure of the TRIPS security exception, contained in Article 73, is similar to that of Article XXI of GATT, and both defensive and offensive hacking cyber operations may be eligible for the exception. Furthermore, to the extent that the availability of Article 73 is self-judging, cyber operations that would otherwise violate TRIPS may be carried out with impunity.

5. International Investment Law

International investment law is drawn partially from customary international law, but is increasingly dominated by bilateral investment treaties (BITs), including the portions of free trade area agreements that are designed to emulate a BIT. BITs generally protect foreign investment originating in the partner country, and sometimes also include market access guarantees providing permission for entry of foreign investment from the partner country.

Often, the market access guarantees are framed as requirements of national treatment with respect to the establishment of the investment. BITs that include these market access guarantees may raise issues regarding whether a host State may exclude certain foreign investors from certain industries in order to carry out a cyber security program, or establish cyber security based conditions for market entry.

In addition, changes in technology or perception result in changes in cyber security concerns that may lead to ejection of, or the imposition of more stringent conditions on, foreign investors. These measures may raise issues under BITs provisions that protect foreign investment from discrimination or mistreatment *after* establishment.

While each BIT is different, some States, such as the US, have model BITs with which they begin negotiations. For purposes of illustration, I will discuss the relevant provisions of the 2012 US model BIT.[27] The national treatment provision of Article 3 of the 2012 US model BIT (National Treatment) provides as follows:

1. Each Party shall accord to investors of the other Party treatment no less favorable than that it accords, in like circumstances, to its own investors with respect to the establishment, acquisition, expansion, management, conduct, operation, and sale or other disposition of investments in its territory.
2. Each Party shall accord to covered investments treatment no less favorable than that it accords, in like circumstances, to investments in its territory of its own

[27] US Department of State, 2012, *U.S. Model BIT*, available at http://www.state.gov/e/eb/ifd/bit/index.htm.

> investors with respect to the establishment, acquisition, expansion, management, conduct, operation, and sale or other disposition of investments.

Note that Article 3(1) provides for national treatment as to establishment – this is a commitment to market access for investment. Article 3 also provides for national treatment for foreign investors and their investments – treatment no less favourable than that accorded to domestic nationals. So, the question raised in connection with cyber security operations is whether exclusions or special conditions applied to foreign investors or their investments would constitute less favourable treatment. Current jurisprudence is somewhat uncertain as to the extent to which differential treatment can be justified in a way that avoids its characterization as 'less favourable.'[28] However, where the different treatment is based merely on different nationality, as opposed to different risk characteristics, it would be unlikely to withstand national treatment scrutiny. Similar issues would arise under the 'most favoured nation' treatment obligation of Article 4, where a State determines to treat foreign investors or investments from different countries differently in connection with cyber security risk.

In addition, Article 5 of the 2012 US model BIT provides that 'each Party shall accord to covered investments treatment in accordance with customary international law, including fair and equitable treatment and full protection and security.' The scope of fair and equitable treatment and full protection and security may impede national defensive cyber activities in connection with foreign investments, for example where a foreign investor or investment is subjected to costly requirements or restraints based on cyber security concerns. While the 2012 US model provides quite restrictive definitions of fair and equitable treatment and full protection and security – referring to due process and police protection – other investment treaties do not restrict the scope of these obligations in this way.

Many BITs include clauses making the protection of essential security interests a defence, justifying an action of the State that would otherwise be prohibited. For example, Article 18 (Essential Security) of the 2012 US model BIT contains the following security exception:

> Nothing in this Treaty shall be construed:
>
> 1. to require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or
> 2. to preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.

[28] See Nicolas DiMascio & Joost Pauwelyn, Non-discrimination in Trade and Investment Treaties: Worlds Apart or Two Sides of the Same Coin, *102 Am. J. Int'l L.* 48 (2008).

Note that this model has a 'self-judging' or subjective feature similar to that found in the WTO provisions. However, most BITs that contain security exceptions do not contain language such as 'that it considers necessary,'[29] with the result that whether a measure is necessary for the protection of the acting State's essential security interests is an objective question, and is not self-judging.

Indeed some BITs do not contain security exceptions at all.[30] Given the concerns described above that defensive cyber operations may violate other provisions of investment liberalization treaties, States may wish to review their policy with respect to the need for security exceptions. Note that where a treaty includes no security exception, a customary international law defence of necessity, based on security needs, may still be available.[31] However, the customary international law necessity defence requires that the non-compliance '(a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.'[32]

By contrast, in Article 3, the OECD *Codes of Liberalisation of Capital Movements and of Current Invisibles Operations,* a legally binding agreement among OECD members but now open to other States, provides that it 'shall not prevent a Member from taking action which it considers necessary for the [...] ii) [...] protection of its essential security interests […].'

A BIT security exception was considered in connection with arbitration cases relating to Argentina's 1999-2002 economic crisis. Article XI of the Argentina-US BIT provides:

> This Treaty shall not preclude the application by either Party of measures necessary for the maintenance of public order, the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security or the protection of its own essential security interests.[33]

Note that this provision contains no indicator that it is 'self-judging,' and indeed the tribunals that considered it indicated that without explicit language making the security exception self-judging, it is not.[34]

---

29 Katia Yannaca-Small, Essential Security Interests under International Investment Law, chapter 5 in *International Investment Perspectives: Freedom of Investment in a Changing World* 93-134, 94 (OECD 2007).

30 *Ibid.* at 98.

31 See the discussion at *ibid.*, 98-100.

32 *cf* International Law Commission, *Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries,* Article 25, United Nations Office for Legal Affairs (2001), available at http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf.

33 *Treaty between the United States of America and the Argentine Republic concerning the Reciprocal Encouragement and Protection of Investment*, signed 14 November 1991, entered into force 20 October 1994, available at: http://www.unctadxi.org/templates/DocSearch____779.aspx.

34 E.g., *CMS Gas Transmission Company v. Argentine Republic*, ICSID Case No. ARB/01/8, Award, 12 May 2005; 29. *LG&E Energy Corp., L&E Capital Corp., LG&E International Inc v. Argentine Republic*, ICSID

In a number of the Argentina cases, the issue came up whether economic crisis could be a basis for invocation of this type of security exception. This question is important to the cyber security issue, because cyber security may also relate to a type of security beyond kinetic warfare. One of the tribunals rejected the argument that Article XI was only applicable in circumstances amounting to military action and war, stating that, to find that a severe economic crisis could not constitute a national security issue was 'to diminish the havoc that the economy can wreak on the lives of an entire population and the ability of the Government to lead.'[35] For the same reasons, this type of provision might be interpreted to be invocable in order to avoid cyber attack based havoc. The Argentina tribunals varied with respect to their interpretation of the degree of severity of disruption that would be necessary in order to invoke the security exception.[36]

6. Conclusion

International economic law was generally not written with cyber operations in mind, and indeed, it generally avoids involvement with security issues. This is the basis for the security exceptions discussed in this chapter, and it is the basis for the political position taken by some States that they will not allow international economic law to restrain their national security-based actions.

However, security exceptions often have some textual limitations as to their availability, and so it is important to review international economic law in order to determine how cyber operations may be restrained. Because negotiators did not have cyber operations in mind when they negotiated international economic law, these rules often do not apply clearly to cyber operations, and there is room for debate and litigation. In a sense, the question of the relationship between international economic law and cyber operations is a type of 'fragmentation' issue, in which one area of international law inadvertently intersects another area of law or policy. It would be possible to enter into a cyber operations specific agreement, and to modify international economic law in order to provide that it defers to the cyber operations agreement, but this would involve difficult negotiations.

Case No. ARB/02/1, Decision on Liability, 3 October 2006; 30. *Enron Corporation Ponderosa Assets, L.P. v. Argentine Republic*, ICSID Case No ARB/01/3, Award, May 22, 2007. *See also Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)*, Merits, 1986 ICJ 14, 116; *Oil Platforms (Iran [Islamic Rep. of] v United States)* 1996 ICJ 803, 20.

35 *LG&E International Inc. v. Argentine Republic*, ICSID Case No. ARB/02/1, Decision on Liability, 3 October 2006, para. 238.

36 See *United Nations Conference on Trade and Development, The Protection of National Security in IIAs*, UNCTAD/DIAE/IA/2008/5, 9-10 (2009).

Jovan Kurbalija

E-Diplomacy and Diplomatic Law in the Internet Era

1. Introduction

In the long history of diplomacy,[1] the development of information and communication technology has profoundly influenced the way representation, negotiations and other diplomatic functions have been conducted. The most important tools in this evolution include the telegraph, the telephone, the radio, the television, and the fax. Each triggered a dynamic interplay of continuity and change in the evolution of diplomacy: continuity in the main functions of diplomacy (the peaceful settlement of disputes) and changes in the way it is performed (the use of new tools). The internet is the latest innovation in this historical evolution.[2, 3] The internet accounts for over 20% of the gross domestic product (GDP) growth in the world's largest economies.[4] With close to three billion users,[5] every third person on this planet is already connected to the internet, and each day over one and a half million people are victims of cyber crime.[6] In developed and developing countries the internet is becoming vital to the functioning of societies and integral to most aspects of daily lives, and it can be deemed the backbone of the global economy.

The internet has profoundly changed information and communication,[7] both of which are pillars of diplomacy. The search for information typically starts with a search engine such as Google or Bing. Wikipedia is often used as an overview of issues and processes, a place to start searching for more detailed information. Our storage banks

1 Almost all early civilisations used some form of proto-diplomacy, including negotiations and the protection of negotiators (immunity). See also: R. Numelin, *The Beginnings of Diplomacy. A Sociological Study of Intertribal and International Relations* (Oxford: Oxford University Press 1950).

2 For more information see *Evolution of technology and diplomacy*, a series of blogs and webinars on the interplay between communication technology and diplomacy, conducted in 2013 by Dr Jovan Kurbalija. <http://www.diplomacy.edu/2013/evolution> accessed 09 November 2013.

3 On the evolution of diplomatic methods see: H. Nicolson, *The Evolution of Diplomatic Method* (London: Constable & Co Ltd, 1954); M.S. Anderson, *The Rise of Modern Diplomacy: 1450-1919* (London: Longman Group, 1939); K. Hamilton and R. Langhorne, *The Practice of Diplomacy* (London: Routledge, 1995); G. Berridge, *Diplomacy: Theory and Practice* (3rd ed., Basingstoke, UK: Palgrave Macmillan, 2005).

4 Pascal-Emmanuel Gobry, 'The Internet is 20% of economic growth' *Business Insider* (24 May 2011) <http://www.businessinsider.com/mckinsey-report-internet-economy-2011-5> accessed 09 November 2013.

5 According to the Internet World Stats on 30 June 2012 there were 2,405,518,376 internet users worldwide. Their data are based on sources from International Telecommunication Union, Nielsen Online, GFK and local ICT regulators, among others. See <http://www.internetworldstats.com/stats.htm> accessed 09 November 2013.

6 W. Jones, 'This Week in Cybercrime: Cybercrime's Industrial Revolution' *IEEE Spectrum* (30 June 2013) <http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-cybercrimes-industrial-revolution> accessed 09 November 2013.

7 cf T. Van Dinh, *Communication and Diplomacy in a Changing World* (Norwood, NJ: Ablex 1987) p.8. ('Communication is to diplomacy as blood is to the human body. Whenever communication ceases, the body of international politics, the process of diplomacy, is dead, and the result is violent conflict or atrophy.').

for documents, emails, and photos have also changed, moving from hard drives to cloud servers. The way we communicate is increasingly shaped by mobile telephones, Skype and other internet tools. The core relevance of information and communication for diplomacy, and the revolution affecting both of them in the internet era, set the stage for the present analysis of the influence of the internet on diplomacy in general and on diplomatic law in particular. It remains to be seen if these changes will trigger just one more evolutionary step in the long history of diplomacy, or if they will catalyse revolutionary change in how, where, and by whom diplomacy is performed. While it will take time for diplomacy to adjust to the internet, some questions require immediate response, as is shown by the revelations of Edward Snowden[8] on PRISM[9] and other internet surveillance activities:[10] how can the protection of diplomatic communication and information be ensured in the era of digital surveillance? Can provisions of the 1961 *Vienna Convention on Diplomatic Relations* (VCDR)[11] remain relevant in the internet era? These and other questions are the subjects of this chapter.

While there are many open questions, the research on the impact of the internet on diplomacy (as on overall society) is in its formative stage. This is reflected by the diverse terminology which has gradually developed. The impact of the internet on diplomacy is very often described as 'e-', 'virtual', 'cyber', or 'digital' diplomacy. Yet while these prefixes describe the same phenomenon – the internet – we tend to use 'e-' for commerce, 'cyber' for crime and war, 'digital' for development divides, and 'virtual' for internet spaces. Usage patterns are starting to emerge. In everyday language, the choice of prefix might be casual but, in internet politics, the use of prefixes has begun to show specific meaning and relevance.

The etymology of the word *cyber* goes back to the ancient Greek meaning of *governing*. 'Cyber' came to our time between the covers of Norbert Weiner's book *Cybernetics*, which deals with information-driven governance.[12] In 1984, William Gibson introduced the word cyberspace in his science-fiction novel *Neuromancer*.[13] The use of the prefix 'cyber' grew parallel to the internet. In the late 1990s, almost anything related to

8 Edward Snowden is former contractor of the US National Security Agency (NSA) who disclosed information about massive surveillance conducted by the NSA and partner institutions. For a series of articles on Edward Snowden see the *Guardian* <http://www.theguardian.com/world/edward-snowden> accessed 18 October 2013.

9 PRISM stands for 'Planning Tool for Resource Integration, Synchronisation, and Management'. PRISM is the NSA's operation aimed at accessing the personal data stored at the servers of US internet companies (Microsoft, Yahoo, Google, Apple, Facebook, Skype, Paltalk, AOL).

10 Other major internet surveillance activities, revealed by E. Snowden, include wiretapping of the internet backbone cables carrying the major internet traffic through two programmes: UPSTREAM performed by the United States National Security Agency (NSA) and TEMPORA performed by the United Kingdom's Government Communications Headquarters (GCHQ).

11 *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

12 N. Weiner, *Cybernetics or Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press, 1965).

13 W. Gibson, *Neuromancer* (New York, NY: Ace Books, 1983).

the internet was 'cyber': cyber community, cyber law, cyber sex, cyber crime, cyber culture etc. In the early 2000s, 'cyber' gradually disappeared from general use, yet it remained alive in security terminology. This is most likely because of the 2001 Council of Europe's *Convention on Cybercrime*, still the only international treaty in the field of internet security.[14] Today, many States issue *Cyber Security Strategies*;[15] the International Telecommunication Union (ITU) has its *Global Cybersecurity Agenda*;[16] the North Atlantic Treaty Organization (NATO) has its *Policy on Cyber Defence*.[17]

'E' is an abbreviation of electronic. Its first and most important use is in e-commerce, as a description of the early commercialisation of the internet. In the European Union's (EU's) Lisbon Agenda (2000),[18] 'e-' was the most frequently used prefix. 'E-' was also the main prefix in the declarations of the World Summit on the Information Society (WSIS, Geneva 2003 and Tunis 2005).[19] [20] WSIS implementation is centred on action lines, including e-government, e-business, e-learning, e-health, e-employment, e-agriculture, and e-science. 'E-' is not as present as it used to be; even the EU has recently abandoned it, trying, most likely, to distance itself from the partial success of the Lisbon Agenda.

Digital refers to 1 and 0 – two digits that form the basis of the whole concept of information and communication technology (ICT) and the internet. Ultimately, all software uses these two digits. In the past, digital was used mainly in development circles to describe the 'digital divide'. In the last few years, however, digital has started conquering the internet's linguistic space. The EU has a 'Digital Agenda for Europe'.[21] The United Kingdom (UK) has digital diplomacy.[22]

---

14 Council of Europe, *Convention on Cybercrime* of 23 November 2001.

15 See a list at NATO CCD COE, *National Strategies & Policies* <http://ccdcoe.org/328.html> accessed 09 November 2013.

16 ITU, *Global Cybersecurity Agenda* <http://www.itu.int/osg/csd/cybersecurity/gca/> accessed 09 November 2013.

17 cf NATO, *NATO and cyber defence*, <http://www.nato.int/cps/en/SID-12A1F016-A72FF943/natolive/topics_78170.htm> accessed 09 November 2013.

18 *Lisbon European Council 23 and 24 March 2000 Presidency Conclusions* <http://www.europarl.europa.eu/summits/lis1_en.htm> accessed 09 November 2013.

19 For the main WSIS declarations and outcome documents see: Geneva 2003 (Geneva Declaration of Principles and Geneva Plan of Action) and Tunis 2005 (Tunis Commitment and Tunis Agenda for the Information Society) <http://www.itu.int/wsis/index.html> accessed 10 November 2013.

20 For the research on the use of prefixes in the WSIS and IGF processes, see DiploFoundation's research project 'Emerging Language of Internet Diplomacy' *Diplo* (Malta, 2013) <http://www.diplomacy.edu/IGFlanguage> accessed 09 November 2013.

21 European Commission, A Digital Agenda for Europe - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (26 August 2010) COM/2010/0245 f/2 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT> accessed 18 October 2013.

22 Foreign Commonwealth Office, *Foreign Commonwealth Office Digital Diplomacy* (no date) <http://blogs.fco.gov.uk/digitaldiplomacy/> accessed 18 October 2013.

An interchangeable use of prefixes can be noticed in the United States (US) State Department which has an *e*Diplomacy department,[23] refers to *digital* diplomacy in the main ICT document and department,[24] and employs a *virtual* embassy to Iran.[25]

The following section depicts the impact of the internet on diplomacy. The third section discusses the status of diplomatic missions in the internet era and the impact of the internet on core diplomatic functions, namely representation, negotiation, protection of nationals, and information gathering. The fourth section provides an analysis of the impact of the internet on diplomatic privileges, immunities, and facilities, and the final section offers some remarks on the future of diplomatic and consular law in the internet era.

2. Impact of the Internet on Diplomacy

The impact of the internet on diplomacy affects three main areas: the changing environment for diplomatic activities, new topics on diplomatic agendas, and new tools for diplomacy.[26]

2.1 The Changing Environment for Diplomatic Activities

The changing *environment* for diplomatic activities refers to the impact of technology on the economy, sovereignty, and concepts of power. Diplomacy does not exist in a vacuum. It is influenced by particular social, political, and economic circumstances. This changing environment for diplomatic activities is affected by the emergence of *defining technologies* that determine economic, social, and political success. They have included – historically – land, population, raw materials, energy, and financial capital.[27] The control of defining technologies has usually meant a strong influence of social and political developments. The defining technology of our era is the information technology, including the internet, with the central importance of knowledge.[28]

---

23 United States Department of State, *Major Programmes of IRM's Office of eDiplomacy* <http://www.state.gov/m/irm/ediplomacy/c23840.htm> accessed 10 November 2013.

24 United States Department of State, *IT Strategic Plan: Fiscal Years 2011-2013 – Digital Diplomacy* <http://www.state.gov/m/irm/rls/148572.htm?goMobile=0> accessed 09 November 2013.

25 United States, *Virtual Embassy of the United States to Iran* <http://iran.usembassy.gov/> accessed 10 November 2013.

26 See also J. Kurbalija, 'The Impact of the Internet and ICT on Contemporary Diplomacy' in P. Kerr and G. Wiseman (ed.) *Diplomacy in a Globalizing World Theories and Practices* (New York: Oxford University Press 2012), 141-159.

27 J.D. Bolter, *Turing's Man: Western Culture in the Computer Age* (London: Duckworth, 1984).

28 cf P.F. Drucker, *The New Realities: In Government and Politics, in Economics and Business, in Society and World View* (Oxford: Heinemann Professional Publishing 1989), p.167. In his description of a knowledge society, Drucker observed that knowledge has become the capital of a developed economy, and that knowledge workers form the group that sets society's trends.

An impact of the defining technologies on diplomacy is illustrated by the level of influence of particular industrial sectors on diplomacy. For example, a few decades ago, the promotion of the interests of the US automobile industry abroad was high on the US diplomatic agenda. Nowadays, the internet industry has more influence on US diplomacy, in both bilateral and multilateral negotiations. Similar trends can be noticed in other countries.

2.2 Internet Governance: A New Topic on the Diplomatic Agenda

New topics are appearing on diplomatic agendas as a result of the growing impact of the internet on modern society. This follows a general trend of extending diplomatic agendas, which David D. Newsom explains as follows:

> For most of the twentieth century, the international diplomatic agenda has consisted of questions of political and economic relations between nation-states — the traditional subjects of diplomacy. After the Second World War new diplomatic issues arose, spurred by the technical advances in nuclear energy and electronics.[29]

Internet-related topics on diplomatic agendas are usually addressed in the context of global internet governance (IG), which includes the following questions: who governs the internet? Who are the actors likely to influence its future development? What will be their policies with regard to connectivity, commerce, content, funding, security, and other issues central to the emerging digital society?

Today, internet governance includes close to 50 policy issues that can be classified in five main groups: infrastructure and standardisation, legal, economic, developmental, and socio-cultural.[30]

Internet governance includes new cyber issues dealing with the proper functioning of the internet (e.g. managing internet names and numbers, net neutrality) and traditional ones whose governance has been affected, or even transformed, by the advent of the internet (e.g. crime, intellectual property, commerce, and privacy protection). Most IG issues are multidisciplinary, combining technical, security, legal, economic, and social aspects.

IG was put on the global diplomatic agenda during the WSIS, which was organised around two main summit events: one in Geneva in 2003 and the other in Tunis in 2005. At the Tunis event, the WSIS established the Internet Governance Forum (IGF) as the

29 D. Newsom, 'The New Diplomatic Agenda: Are Governments Ready?' *International Affairs* (January 1989) p.29.

30 J. Kurbalija, *An Introduction to Internet Governance* (Malta: DiploFoundation, 2011), pp. 27-29.

main global body which addresses the governance of the internet in a holistic way.[31] The establishment of the IGF was a result of a compromise between government-centred and non-governmental approaches to IG (the so-called 'Tunis compromise'). The government-centred approach, promoted predominantly by developing countries, argued that the internet should be governed by international organisations under the United Nations (UN) umbrella. The non-governmental approach, favoured by developed countries and in particular by the US, argued for a preservation of existing IG with the close involvement of the business sector and civil society.

The 'Tunis compromise' has been increasingly challenged. First, at the World Conference on International Telecommunications (WCIT)[32] in Dubai in December 2012, an attempt was made to increase the ITU's involvement in managing internet-related matters. The result was polarised votes at WCIT, mainly along the lines of developed/developing countries.[33] Second, the revelations of massive internet surveillance re-energised discussion on the future institutional framework for IG. In the forthcoming period a series of events will take place at which the future institutional arrangements for IG will be discussed. Following a joint initiative by the Internet Corporation for Assigned Names and Numbers (ICANN) and Brazil, Brazil will host the Global Multistakeholder Meeting on the Future of Internet Governance (Sao Paolo, 23-24 April 2014), aimed at discussing universal internet principles and future IG institutional arrangements.[34] In 2015, the WSIS +10 events are likely to be dominated by discussions on the future of IG, including the future role of the IGF.[35]

2.3 New Tools for Diplomacy

As it did with other professions, the internet brought new tools to diplomacy. E-mail is now the main communication tool used in diplomatic services. Diplomats use search engines to find information, and increasingly use teleconferencing, social media, and other ICT and internet tools. These technologies impact the way modern diplomacy operates. The internet introduced new means of conducting diplomacy. Diplomatic signals are sent via Twitter and blogs. Resolutions and other diplomatic texts are drafted using Google Docs and other online drafting tools.

---

31 See Tunis Agenda for the Information Society (Articles 72-78) <http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf > accessed 10 November 2013.

32 See <http://www.itu.int/en/wcit-12/Pages/default.aspx>.

33 89, mainly developing, countries voted for amendment of the International Telecommunication Regulations (ITR); 55, mainly developed, countries voted against the proposed amendments of the ITR.

34 See <http://www.brasil.gov.br/governo/2013/11/brasil-vai-sediar-conferencia-sobre-governanca-na-internet>.

35 The first WSIS summit meeting took place in 2003. The reviews of the WSIS are collectively called WSIS+10, although there is no specific schedule or agenda for the process. For a news article announcing the 'start' of the process, see <http://www.ifla.org/news/start-of-wsis10-review-meeting-at-unesco-hq-in-paris-france> accessed 10 November 2013.

3. Diplomatic Law

Diplomatic law covers three main areas: (1) the establishment of diplomatic relations and the status of diplomatic missions; (2) the performance of diplomatic functions; and (3) diplomatic immunities, privileges, and facilities. Diplomatic law has developed gradually through the crystallisation of practices, and the creation of customary rules. The codification of customary diplomatic law started at the Congress of Vienna (1814–1815) when the rule of diplomatic rank and order of precedents[36] were codified in the *Vienna Regulation* of 1815. This was followed by the 1928 *Havana Convention on Diplomatic Officers*[37] and the *Harvard Research Draft Convention on Diplomatic Privileges and Immunities* of 1932.[38] After World War II, two main instruments were adopted to regulate the diplomatic status of the international organisations: the *Convention on the Privileges and Immunities of the United Nations* of 1946[39] and the *Convention on the Privileges and Immunities of Specialised Agencies* of 1947.[40] The latest comprehensive codification of diplomatic law was conducted by the 1961 *Vienna Convention on Diplomatic Relations* (VCDR)[41] which deals with the status and functioning of diplomatic missions exchanged by States. With 187 State parties and a high level of adherence, the VCDR is considered to be one of the most successful international legal instruments. Violations of the provisions, as in the case of Iran taking US diplomats hostage in Teheran (1979–1981) are rare. As the International Court of Justice (ICJ) indicated in the *Teheran Hostage* case, diplomatic immunities are 'essential for the maintenance of relations between States and are accepted throughout the world by nationals of all creeds, cultures and political complexions'.[42]

The VCDR deals with the status and functioning of the diplomatic missions exchanged by States, which are, together with consular relations, the traditional and main features of diplomatic services. However, twentieth century diplomacy extended beyond bilateral diplomatic relations through the exchange of two States' embassies and consulates. The

36 An 'order of precedence' is a hierarchical list of diplomats and other dignitaries. It is used for seating arrangements at events and such occasions attended by diplomats and other officials. Order of precedence was a sensitive issue prior to the Congress of Vienna. It was the cause of tension among diplomats, including conflicts among States. The Vienna Regulations of 1815 established rules, order, and stability in this field.

37 The Havana Convention, to which 14 South American States became party, was an interim solution for the lack of rules in this field. It codified some regional customs, such as diplomatic asylum, which remains specific to this region. See <http://www.oas.org/Juridico/english/sigs/a-25.html> accessed 10 November 2013.

38 The 'Harvard Convention' was a private codification which made significant impact on the subsequent codification of diplomatic law. More information on the codification can be seen C. E. Baumann, *The Diplomatic Kidnappings: A Revolutionary Tactic of Urban Terrorism* (The Hague, Netherlands: Martinus Nijhoff, 1973) p.37.

39 *Convention on the Privileges and Immunities of the United Nations*, 1 U.N.T.S. 15.

40 *Convention on the Privileges and Immunities of the Specialized Agencies*, approved by the General Assembly of the United Nations on 21 November 1947, see <http://www2.kobe-u.ac.jp/~nmika/linked_files/Special_Lecture2010/Treaties/Convention_Priviledges_Immunties_Specialized_Agencies.pdf> accessed 10 November 2013.

41 *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

42 ICJ, *Case concerning United States Diplomatic and Consular Staff in Tehran,* Judgment, I.C.J. Reports 1980, p.3, para. 86.

main development was the fast growth of multilateral diplomacy, especially since 1945, with new forms of representation of States via permanent missions, and the need to regulate the diplomatic status of international organisations and their officials.[43]

These developments triggered the adoption of other diplomatic law conventions based on the provisions of the VCDR: the 1963 *Vienna Convention on Consular Relations* (VCCR),[44] the 1969 *Convention on Special Missions* (CSM), and the 1975 *Convention on Relations of States with International Organizations* (CRSIO).[45] In addition to these core instruments, diplomatic law also includes the 1977 *Convention on the Prevention and Repression of Offences against Internationally Protected Persons including Diplomats*.[46] The main focus of the present analysis will be the VCDR. Reference will be made to other conventions when they differ from the VCDR regulations.

3.1 Status and Organisation of Diplomatic Relations

According to Article 2 of the VCDR,[47] the process of establishing diplomatic relations between States is a matter of agreement between the governments concerned. Typically, diplomatic relations follow mutual recognition of two countries, especially after the newly declared independence of one of them. Establishing diplomatic relations does not require the opening of diplomatic missions in the respective capitals. In fact, many countries, due to limited human and financial resources, cannot maintain an extensive network of diplomatic missions. For example, Malta has diplomatic relations with 162 countries which are covered by 25 resident diplomatic missions (embassies and high commissions),[48] 19 non-resident ambassadors based at regional hubs (e.g. Japan is covered from the embassy in Beijing), and 13 non-resident ambassadors based in the capital (Valletta).[49, 50]

---

43 In addition, new actors in global diplomacy have emerged, with claim to be recognised as diplomatic actors: special envoys, regional/local entities, rebel groups, and civil society, among others.

44 *Vienna Convention on Consular Relations*, 596 U.N.T.S. 8638.

45 *Convention on Relations of States with International Organizations*, UN Doc. A/CONF.67/16 (14 March 1975).

46 *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents*, 1035 U.N.T.S. 167.

47 *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

48 Malta also has seven permanent missions to international organisations.

49 For an analysis of diplomatic challenges of small States see 1. V. Camilleri, *How Small States Influence Diplomatic Practice: A Look at The Fourth Round of Accession Negotiations to the European Union* (Paper presented at the International Conference on the Diplomacy of Small States, Malta, 8-9 February) <http://www.diplomacy.edu/poolbin.asp?IDPool=357> accessed 18 April 2013.
2. A. Henriksen, 'Diplomacy and Small States in Today's World' in *The face of man, Vol. 2, The Dr. Eric Williams Memorial Lectures 1993 – 2004* (Trinidad and Tobago: Central Bank of Trinidad and Tobago, 2005) <http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3224> accessed 18 April 2012.
3. A.N. Mohamed, 'The Diplomacy of Micro-States' (Clingendael Discussion Papers in Diplomacy, No. 78. 2002) <http://www.clingendael.nl/publications/2002/20020100_cli_paper_dip_issue78.pdf> accessed 18 April 2012.

50 Data from the website of the Maltese Ministry of Foreign Affairs, <http://www.foreign.gov.mt/default.aspx?MDIS=741> accessed on 11 November 2013.

The trend of finding new ways of maintaining diplomatic relations is driven by pressures to reduce government expenditures, including expenses for diplomatic services. New innovative ways that increasingly rely on the intensive use of digital tools have been emerging. One is the use of missions in multilateral posts as hubs for a range of diplomatic or consular activities that cannot be conducted bilaterally (e.g. permanent missions to the UN in New York are used for this purpose by many small States). A second is the use of regional hubs to cover countries in the region (e.g. the ambassador in New Delhi could cover Southern Asian countries as a non-resident ambassador). A third innovative practice is diplomatic coverage from the capital, via a non-resident, so called 'roving', ambassador (this practice of using a roving ambassador is often referred to as the 'Scandinavian model', as it was first endorsed by Sweden). A fourth is the use of honorary consuls, recruited from the expatriate population, or even extra-national, cultural, business, or professional communities. A fifth is contracting some services, either from friendly nations (e.g. consular services) or from specialised private operators (e.g. lobbying activities).

Today's information and communication technologies are opening up a sixth alternative – that of virtual embassies, i.e. embassies that do not have physical premises. A virtual embassy would still have an ambassador. In a *real* embassy, the ambassador resides (physically) in the embassy located in the territory of the receiving State. In a *virtual* embassy, the ambassador would remain in the capital city of his or her own country and communicate with the other country by electronic means.

The experiments with virtual embassies led in two directions. First, the technology-driven approach led towards establishing virtual embassies on Diplomacy Island of Second Life, an online virtual world. The first example was the virtual embassy of Maldives[51] followed by Sweden, Estonia, the Philippines, Macedonia and Columbia. These virtual embassies were virtual reality replicas of real buildings with the possibility of interacting with cyber diplomats. This experiment has not been developed further, mainly due to the limitations of Second Life as an internet platform. Second, a function-based approach built virtual embassies as websites. For example, the US has 40 Virtual Presence Posts established to 'improve our engagement with specific communities where the U.S. has no physical diplomatic facilities'.[52] In December 2011 the US established a completely virtual embassy in Iran, a country where it has no physical diplomatic representation.[53]

---

51 B. Muralidhar Reddy, 'Maldives opens "virtual embassy"' *The Hindu* (25 May 2007) <http://www.thehindu.com/todays-paper/tp-international/maldives-opens-virtual-embassy/article1847030.ece> accessed 10 November 2013.

52 Major Programs of IRM's Office of eDiplomacy' (U.S. Department of State, 2013) <http://www.state.gov/m/irm/ediplomacy/c23840.htm> accessed 10 November 2013.

53 The US interests in Iran are protected by the Swiss embassy in Teheran. The US virtual embassy to Iran is located at <http://iran.usembassy.gov> accessed 10 November 2013.

The interplay between new technological developments, especially in the field of virtual reality, and the need to perform diplomatic functions in a more effective way, will affect the future of 'virtual embassies'. It is very likely that virtual embassies will be used for 'blended diplomatic representation' by using virtual tools for maintaining contact between the visits of non-resident ambassadors ('roving' ambassadors). Blended representation could combine the best of the two forms of representation: traditional (physical contact, developing personal rapport) and online (low cost, continuous communication).

3.2 Core Diplomatic and Consular Functions in the Internet Era

Scholarly writings provide numerous classifications of diplomatic functions. The classification used in this chapter is based on Article 3 of the VCDR which depicts the following diplomatic functions as:

(a) representing the sending State in the receiving State;
(b) protecting in the receiving State the interests of the sending State, and of its nationals, within the limits permitted by international law;
(c) negotiating with the Government of the receiving State;
(d) ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State; and
(e) promoting friendly relations between the sending State and the receiving State, and developing their economic, cultural and scientific relations.

3.2.1 Representation

From the earliest days, representation has been a vital function of diplomacy. Representation involves speaking and acting on behalf of the sending State. Formally, it includes participation in the official functions of the receiving State on behalf of the sending State. Such participation is a sign of goodwill, and can enhance further relations between the sending and the receiving States. Accordingly, Costas Constantinou defines diplomacy through communication and representation: 'At its basic level, diplomacy is a regulated process of communication between at least two subjects, conducted by their representative agents over a particular object.'[54]

The most common form of representation, through resident diplomatic missions, has already been challenged by several emerging practices.[55] However, driven by technological advances, questions arise about what impact the internet will have on diplomatic representation, and whether the official websites of the Ministries of

54 C. M. Constantinou, *On the Way to Diplomacy* (Minneapolis USA: University of Minnesota Press, 1966) p.25.
55 See section 3.1.

Foreign Affairs (MFAs) and diplomatic missions can be deemed another form of State representation.

Websites currently provide the main presence of diplomatic services on the internet. There is a considerable number of diplomatic websites, including approximately 150 MFA websites, and more than 3000 diplomatic and consular mission websites. Most MFA websites offer basic foreign policy texts, press releases, a *who's who* of the MFA, travel information, information for foreigners and more. Initially, websites were created as internet versions of the traditional one-to-many diplomatic communication, but they are now shifting towards more interactive communication through integration with social media such as blogs and Twitter.

If a State's official website is its representation on the internet, this raises many questions about the way in which diplomatic representation is conducted. For example, what is the legal status of the US virtual embassy to Iran, and other web-based representations introduced under the Virtual Presence Points programme? Could the internet blocking of the website of the US Virtual embassy to Iran be considered a refusal to accept this type of diplomatic relations? The practice of virtual representation could contribute to the increasing invalidation of Article 41(2) of the VCDR, which specifies that '[…] all official business [...] shall be conducted with or through the Ministry of Foreign Affairs […]'. This paragraph has already been rendered obsolete by the practice of modern diplomacy, in which diplomats communicate directly with various ministries and individuals in the receiving country. The use of official websites for representation could further bypass this norm.

Another important aspect of diplomatic activities on the internet is the relevance of online content to the development of international customary law. Currently, it is not clear whether information published on a website or Facebook page can be considered an official statement by a ministry, and therefore, a possible indication of an *opinio iuris* of, and/or contribution to, the establishment of consistent practice by a State, these aspects being preconditions for the development of international customary rules. So far, there are no examples of the use of online communication as supporting evidence for the development of international customary law.

With online presence, diplomatic services are also more exposed to potential fraud that could endanger their representation roles. As an example, in 2011 the Indian Consulate General in Geneva published a notice in the *International Herald Tribune*, advising the public about a fraudulent website using the consulate's name.[56] What can the Indian government do in a situation such as this? Can India force the takedown of the fake website of the Indian Consulate in Geneva and, if so, through what means? If the

[56] Although the article in the *International Herald Tribune* is no longer accessible, a scan of the public notice can be seen at <http://deepdip.wordpress.com/2011/12/03/internet-fraud-in-diplomacy/> accessed 09 November 2013.

fraudulent website is registered under the '.ch' domain, the government of India may take action based on Article 28 of the VCCR and request the receiving State to provide 'full facilities for the performance of the functions of the consular post'. The closest analogy to the 'real' world would be that India would demand the closing of any building which falsely claimed to be the Indian Consulate General. But in the online world, this is not likely to be effective. Governments cannot just order national internet registrars to remove a website. If the fraudulent website were registered under a generic domain (.com, .org, .net), the situation would be even more complicated, since the responsible registrars might be located abroad, under foreign jurisdiction. The possibility for legal action, even at the level of theoretical speculation, is almost non-existent.[57]

3.2.2 Protection of Nationals and Consular Assistance

The protection of nationals, and consular assistance, deal with defending or safeguarding any assets or interests of the sending State and its nationals (as well as their assets and interests) from disadvantageous consequences (or from disadvantageous situations, actions, or injuries).

Consular assistance focuses mainly on the protection of interests and the wellbeing of nationals of the sending State. From once being the 'Cinderella' of traditional diplomacy,[58] consular protection has evolved into the recognition that it is a vital part of diplomatic services.[59] The current relevance of consular activities was catalysed by growing public demand for the protection of citizens, and effective response to crises. Easier and more affordable travel, in particular air transport, increased citizens' mobility and their need for consular protection. With instant social and traditional media coverage, natural and political crises worldwide became part of domestic politics. The protection of nationals caught in a crisis easily garners high media and political visibility. MFAs are under increasing pressure to provide more services with limited resources. This tension is probably why the consular field has been an area of many innovations in diplomacy, including the introduction of e-visas, the strengthening of the role of honorary consuls, and the use of social media for communication with nationals.

For example, social media has proven to be highly effective in crisis situations. A crisis situation, natural or political, affects a broad range of people, and communication is an essential part of dealing with it. Faced with danger, people organise themselves by using all available e-tools, including mobile phones, Twitter, and Facebook, very often

57 J. Kurbalija, 'Internet Fraud in Diplomacy' (Reflections on Diplomacy, 03 December 2011) <http://deepdip.wordpress.com/2011/12/03/internet-fraud-in-diplomacy/> accessed 10 November 2013.

58 M. Heijmans and J. Melissen, 'Foreign Ministries and the Rising Challenge of Consular Affairs: Cinderella in the Limelight' in K. S. Rana and J. Kurbalija (eds), *Foreign Ministries: Managing Diplomatic Networks and Optimizing Value* (Malta: DiploFoundation, 2007) pp.192–206.

59 For a long time, consular activities have been considered less important than diplomatic ones. In MFAs, the main career path was related to bilateral and multilateral diplomacy. Consular activities started regaining relevance in recent years.

in innovative ways. In the case of natural disasters, notable examples include the Asian tsunami (2004) and the earthquakes in Chile (2010)[60] and Haiti (2010).[61] In political crisis situations, an example of the prominent use of e-tools was the Arab Spring (2010-2011).[62] These examples demonstrate an essential role for social media in diplomatic services, whether diplomats are involved in humanitarian assistance, in support for their citizens, in conflict prevention, or in other situations.

Further, the internet and social media have revolutionised the relationship between the diaspora and their home country. Previously sporadic contact has evolved into more regular interaction. In this time of financial crisis, with the growing importance of remittances, the migrants' role in the political and social life in their home country has been increasing in importance. The use of social media for connecting the diaspora provides a lot of opportunities. It is still an underused area of e-diplomacy, although there are some examples of its use, such as the extensive use of Facebook by the US and the UK to connect with expatriates, both for disseminating information and for providing a forum for conversation.[63]

The use of social media in this field has raised some new controversies. One illustrative case was the reporting by the US Embassy in Beijing on air-pollution based on data collection by air-sensors at the Embassy premises.[64], [65] Chinese officials said that such practice breached Article 41 of the VCDR which requires that diplomats should act in accordance with the laws of the receiving State and conduct their official business via the MFA.[66] US officials replied by shifting discussion from the diplomatic to the consular field. They justified the sharing of air-pollution data on the basis of assisting

60 'Twitter tells the real-time story of the quake's human toll' *France 24* (28 February 2010) <http://www.france24.com/en/20100227-twitter-disaster-info-chile-earthquake-america-south-tsunami-internet> accessed 11 November 2013.

61 'Twitter Helps in Haiti Quake Coverage, Aid' *The Wall Street Journal* (14 January 2010) <http://blogs.wsj.com/digits/2010/01/14/twitter-helps-in-haiti-quake-coverage-aid/> accessed 11 November 2013.

62 'Facebook, Twitter Help the Arab Spring Blossom' *Wired Magazine* (16 April 2013), <http://www.wired.com/magazine/2013/04/arabspring/> accessed 11 November, 2013.

63 See, for example, the 'UK in Bahrain' – Facebook page <https://www.facebook.com/ukinbahrain/> accessed 18 October 2013.

64 J. Kurbalija, 'Is tweeting a breach of diplomatic function?' *Diplo* (Malta, 2012) <http://www.diplomacy.edu/blog/tweeting-breach-diplomatic-function#_ftn1> accessed 17 October 2013.

65 K. Bradsher, 'China asks other nations not to release its air data' *N.Y. Times* (2012) <http://www.nytimes.com/2012/06/06/world/asia/china-asks-embassies-to-stop-measuring-air-pollution.html?_r=3&> accessed 17 October 2013.

66 China's reaction reflects its cautious approach to, and potential dilemmas with, the position of diplomats in the internet era. The complaint was lodged by the Vice-minister for the Environment, not the MFA. Usually, in the case of a breach of the Vienna Convention (1961) protests are lodged by diplomatic note, or in more extreme cases, by declaring foreign diplomat(s) *persona non grata* (in this case, the US environmental representative, perhaps?). The Chinese authorities decided to send a diplomatic signal (i.e. express uneasiness) without escalating the conflict, see Kurbalija, *supra* note 64.

American citizens in China, something they are entitled to do according to Article 5 of the VCCR.[67]

3.2.3 Negotiation

Negotiation is considered the main function of diplomacy both in bilateral and in multilateral diplomatic relations. Quincy Wright defines diplomacy as 'the art of negotiation, in order to achieve the maximum of group objectives with a minimum of costs, within a system of politics in which war is a possibility.'[68] Hedley Bull defines diplomacy as 'the management of international relations by negotiations.'[69] While the function of negotiation – reaching agreement – involves important human input based on particular skills and talents, many activities surrounding multilateral and bilateral negotiations are of a routine nature and appropriate for automation. The process of multilateral negotiation can be highly automated through the use of online tools to facilitate logistical support, distribute materials, and to enable the participation of non-governmental organisations and others. In this context, online tools cannot alter the actual negotiating methods, but they can change the environment in which the negotiation is prepared and conducted.

The first major use of computers in an international negotiation was at the Earth Summit in Rio de Janeiro (1992), where mailing lists were used to follow the negotiations and engage the global community. The use of mailing lists was further developed at major UN conferences on human rights (1993), population (1994), women (1995), and social development (1995). However, the main breakthrough in the use of the internet came during the WSIS meetings in 2003 and 2005, and at IGF meetings, which have been held annually since 2006. Perhaps the reason for this breakthrough is that it seemed logical that negotiations discussing the internet should use the internet as a tool. The WSIS and IGF meetings set new standards in e-diplomacy and inspired the use of new e-tools in other areas of multilateral negotiations, such as climate change, migration, and human rights.

During the WSIS, the internet was available in conference rooms, through the widespread use of wireless technology ('wireless fidelity' – WiFi, also known as 'wireless local area network' – WLAN). It made international negotiations more inclusive and open through the participation of an increased number of civil society and business sector representatives, including those who could not, for financial or other reasons, physically

67 Article 5 of the *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

68 Q. Wright, 'The Role of International Law in Contemporary Diplomacy' in S.D. Kertesz and M.A. Fitzsimons (eds.), *Diplomacy in a Changing World* (Indiana, USA: University of Notre Dame) p.55.

69 H. Bull, *The Anarchical Society: A Study of Order in World Politics* (New York: Columbia University Press 1977) p.162.

participate in the meetings,[70] as they began to participate online. For diplomats at the WSIS and IGF meetings, the WiFi connection provided constant contact with their MFAs and other government departments dealing with WSIS issues. In some cases, a WiFi network of notebooks enabled the coordination of initiatives among representatives physically present in a conference room. Exchanges of SMSs, tweets, and emails complemented and sometimes replaced the traditional ambiance of short chats between diplomats from different countries, *tête-à-tête* exchanges, and corridor diplomacy. Because physical movements can reveal the dynamics of negotiations or even form part of diplomatic signalling, this aspect of *in situ* diplomatic negotiation started changing with the use of the internet in conference rooms.[71] The experience from WSIS and the IGF meetings also shows that, despite all the promises of virtual conferencing and other multimedia technologies, today – even more so than in the past – text remains diplomacy's central tool. Most exchanges between preparatory sessions are done via mailing lists and e-mail. The IGF is supported by very active social media discussions, using text-intensive tools, such as discussion lists, blogs, and Twitter.[72]

Another development which highlights the relevance of text is the emergence of verbatim reporting at IGF meetings. This development may have a substantive impact on multilateral diplomacy and negotiations. Verbatim reporting is the process whereby all verbal interventions are transcribed simultaneously by special stenographers and immediately displayed on a large screen in the conference room, as well as broadcasted via the internet. [73] While delegates are speaking, transcripts of their speeches appear on the screen. Verbatim reporting has had an important effect on the diplomatic *modus operandi*. The awareness that what is said will be preserved in print, makes many participants more careful in choosing the level and length of their verbal interventions. Verbatim reporting also increases the transparency of diplomatic meetings.

Additionally, the internet has potential applications in the conversion of verbal agreements to a written format; this is one of the crucial phases in the negotiation process. Group editing applications enable negotiators to work collaboratively on a text by changing the text and adding comments.

The use of new e-tools for negotiation should be approached carefully, and within appropriate contexts. Diplomacy is a profession that often requires discretion. While openness is the guiding principle of good governance, reality shows that most of the successful diplomatic deals have been done discretely, far removed from the public

70 J. Kurbalija, 'World summit on Information Society and the Development of Internet Diplomacy' in M. Gatt and R. Fsadni Azad (eds.), *Governing the Internet* (Malta: Academy for the Development of a Democratic Environment, 2011) ch. 2 <http://thinkingeurope.eu/sites/default/files/publication-files/governing_the_internet.pdf> accessed 10 November 2013.

71 *Ibid*.

72 Kurbalija, *supra* note 30.

73 Kurbalija, *supra* note 26, p.152.

eye.[74] There are many reasons why negotiations should be discreet. Sometimes, discreetness is needed to protect the interlocutor on the other side of the table.[75] In many cases negotiators spend a lot of time finding face-saving formulas for the audience back home.[76] Discreetness usually helps to prevent effective negotiations from turning into a show for the general public. It should be borne in mind that the core of diplomacy is not popular in many societies, especially when it is contrasted with national interest, pride, and glory. Reaching a compromise and maintaining discretion in negotiations are very often closely linked.[77] This considered, it is easy to envisage negotiations that could not be conducted efficiently in front of web cameras. The decision whether to use technical tools for negotiation will be probably in itself part of the negotiation.

Most procedures for diplomatic negotiations are drafted for an event where negotiators are present in the same physical location. Online tools provide the possibility for remote participation. They open a new set of procedural and legal questions: can remote participation be considered the same as *in situ* participation? Can negotiating parties submit amendments online?[78] Is online voting the same as *in situ* voting? Since the use of e-tools is both a reality and a necessity in modern diplomatic negotiations, legal and procedural questions will have to be addressed either by introducing amendments to existing procedural rules or developing new rules and practices.

3.2.4 Information Gathering

Information gathering is a traditional diplomatic activity listed in the VCDR and in most definitions of diplomacy. While information was a scarce resource throughout history, the current period is characterised by the massive production of information in electronic formats. The former difficulty of obtaining information has, to a large extent, been replaced by the challenge of managing, validating and processing what is now available. This abundance of information is as problematic as scarcity once was: important information can be lost in sheer quantity. Fast and precise access to necessary information is *conditio sine qua non* of the proper functioning of an MFA and other participants in foreign policy.

Over the last ten years, diplomats have shifted from relying on internal, mainly traditional, resources to relying on information available outside diplomatic services, mainly on the internet. Sophisticated search engines such as Google, Bing and Yahoo! have made possible precise and timely access to needed information. Diplomats also

74 *id*, 'How will Wikileaks affect diplomacy?' *Diplo* (Geneva, 1 December 2010). <http://www.diplomacy.edu/blog/how-will-wikileaks-affect-diplomacy> accessed 09 November 2013.

75 *Ibid*.

76 *Ibid*.

77 *Ibid*.

78 Some of these issues have been already discussed in the organisations that are the most advanced in using online tools, such as the International Telecommunication Union.

often use new services such as Wikipedia, a web-based encyclopaedia with over 13 million articles written in many languages by contributors around the world, as a starting point and orientation, before continuing to more in-depth research.[79] It is very relevant for diplomats because, in most cases, it provides complete and up-to-date coverage of main diplomatic events and policy developments. Very often, Wikipedia contains first-hand information from people on the spot. Only a few large diplomatic services can provide coverage of international events comparable to Wikipedia. Of course, it is necessary to verify information from Wikipedia while comparing it with information from other sources. The blogosphere is another highly relevant source of information and opinion available for diplomats. Unlike anonymous Wikipedia articles, blogs are attributed; some blogs are written by respected and influential authors. Blogging as a media channel is now a well-established and recognised communication tool. Today there are more than 100 million blogs with often informal, but well-established, ranking procedures.[80] Blogs are particularly influential in specialised policy fields such as climate change, migration, and food security. They influence policy and agenda-shaping in international negotiation. Another emerging approach is to combine access to open data with advanced data-mining techniques. New policy insights could be gained by accessing previously unrelated data in a new context.

The Snowden revelations of the information surveillance of embassies and missions put in focus the difference between lawful and clandestine information gathering, as well as between diplomacy and intelligence. The former British diplomat Sir Reginald Hibbert provided the following breakdown of information gathering in diplomacy:[81] (1) 90% of information is gathered by using lawful means, of which 50% is gathered from public sources; 10–20% from confidential contacts of diplomats; 20–25% from leaks and indiscretion; (2) 10% of information is obtained through covert and clandestine operations, usually referred to as intelligence.

These two main ways of gathering information lead to a complex interplay, and even tension, between diplomacy and intelligence. Intelligence has been developing rapidly since the nineteenth century when many European countries established a so-called *cabinet noir* within their secret police for surveillance of foreign diplomatic correspondence.[82] Intelligence gathering grew in strength during the two World Wars and during the Cold War, and started competing with diplomacy. As described by

79 Wikipedia <http://www.wikipedia.org> accessed 17 October 2013.

80 See for an example of a blog ranking 'Technorati Top 100' (Technorati 2013) <http://technorati.com/blogs/top100/> accessed 09 November 2013.

81 Hibbert's information source breakdown was prepared in the 1990s before the explosive growth of the internet. It is very likely that the importance of public sources has increased, especially with new possibilities of generating intelligence through the use of data-mining tools. R. Hibbert, *Intelligence and National Security* (London: Hodder and Stoughton, 1990) p.112.

82 K. Hamilton and R. Langhorne, *The Practice of Diplomacy* (London: Routledge, 1995), pp.122-124.

Hibbert, 'secret intelligence, from being a somewhat bohemian servant and associate of the great departments of state, gradually acquired a sort of parity with them.'[83]

Diplomacy and intelligence are two closely related but separate functions of a State's foreign affairs apparatus. They involve different methods, institutional frameworks, and skills. The overlap between diplomacy and intelligence exist when an intelligence officer uses a diplomatic cover by acting as diplomatic staff. Intelligence officers get diplomatic titles in order to benefit from diplomatic protection and immunities.[84] Diplomacy and intelligence increasingly compete for resources and influence with policymakers.

The VCDR draws a clear dividing line between diplomatic and intelligence functions. Article 3(1) specifies that diplomats should acquire information *by all lawful means*.[85] Information gathering by diplomats can be conducted in a confidential way, but it should not be clandestine (espionage) and illegal. This distinction is particularly important when clandestine operations become public, as through the recent revelations about the US National Security Agency (NSA) surveillance by the whistleblower Edward Snowden. The public knowledge of such operations could trigger questions of State responsibility for a breach of the VCDR. It could be also a reason why both US and UK authorities have been expressing general regret, while avoiding specific apologies to officials or countries allegedly targeted by the surveillance operation. Such apologies could be tacit official confirmations of such practice that could trigger use of international legal remedies by the affected countries.

Snowden's recent revelations include cases of surveillance of diplomatic communications at the G20 meeting in London in 2009,[86] the offices of 38 diplomatic missions in the US[87] and the Heads of State of Brazil and Mexico.[88] This brings into focus the ever persistent question of acceptable ways of acquiring information. Intelligence gathering was always part of diplomatic practice. However, the VCDR clearly outlawed intelligence gathering which does not use 'lawful means'. There are also strong elements for arguing that international customary law prohibits surveillance of a Head of State or Government. The protection of the secrecy of diplomatic communication and the impact of the

83 Hibbert, *supra* note 81, p.114.

84 During the Cold War, it was typical to have massive expulsions of Soviet Union and Western diplomats, who were intelligence officers working under diplomatic cover. One of the largest was the expulsion of 105 Soviet diplomats from London in 1971.

85 The VCCR is more specific than the VCDR by indicating in Article 5 that 'by all lawful means' refer to 'commercial, economic, cultural and scientific life of the receiving state'.

86 E. McAskill, N. Davies, N. Hopkins, J. Borger J. Ball, 'GHCQ interception foreign politicians' communications at G20 summit' *The Guardian* (16 June 2013) <http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits> accessed 17 October 2013.

87 *Ibid*.

88 V. Bevins and T. Wilkinson 'New Snowden documents allege US spying on Brazil, Mexico' *LA Times* (2 September 2013) <http://articles.latimes.com/2013/sep/02/world/la-fg-wn-ff-snowden-spying-brazil-mexico-20130902> accessed 17 October 2013.

Snowden revelations on diplomatic immunities and privileges will be discussed *infra* in more detail (section 4.3.2).

3.2.5 Diplomatic Reporting

The internet has definitely affected diplomatic reporting. It has made it more effective, more immediate, more cost-effective, and less formal. In the past, diplomats competed with journalists to obtain current news. In the late 1990s, a shift occurred with real time coverage of world events 24/7 (so called 'CNN effect'). The next shift in diplomatic reporting came with the emergence of Wikipedia and social media, which further focused diplomatic reporting on analysis and evaluation that cannot be otherwise found on the internet.

Their constant connectivity with their capital has also made diplomats more present in decision-making processes back home. This is augmented by a ready access to the aggregated knowledge and experience of their colleagues and their counterparts via wikis, blogs, and information aggregators. That, for example, an expert on Asian affairs can be called to the table quickly to give an opinion on a crucial matter, or indeed that the diplomatic circle of knowledge is expanding to include academics and other subject-matter professionals, can only better serve the cause of diplomatic analysis and reporting.

A recent survey of 105 diplomats from five regions (the Americas, Europe, Africa, the Middle East, and Asia) shows the major impact of the internet on diplomatic reporting.[89] The vast majority claimed that it has made their work more effective, more immediate, more cost-effective, less formal, and more pressurised (see Table 1).

No change	Less	More	
4%	5%	91%	Effective
6%	1%	92%	Immediate
5%	9%	86%	Cost effective
9%	84%	6%	Formal
17%	20%	63%	Pressurised

Table 1. How has the internet affected diplomatic reporting?

[89] M. Murphy, 'How has the Internet affected diplomatic reporting?' *Diplo* (Malta, 01 July 2013) <http://www.diplomacy.edu/blog/how-has-internet-affected-diplomatic-reporting> accessed 17 October 2013.

4. Immunities, Privileges and Facilities

The provisions of the VCDR and related diplomatic conventions regulate the aspects of immunities, privileges, and facilities. While these three concepts are sometimes used in overlapping ways in practice, the VCDR distinguishes between them as follows:

- Immunities are exemptions from the jurisdiction of the foreign State. Immunities include inviolability, the giving of evidence, and the execution of judgements in civil proceedings. In practice, a distinction is made between immunities granted to entities, organs, and their premises; immunities granted to diplomats and their dependents; and immunities granted to their activities.
- Privileges refer to the exemption from certain laws and regulations of the receiving State. These are privileges to the extent that others, especially the citizens of the receiving State, do not enjoy. Exemption from taxation by the receiving State is another example of diplomatic privileges. Others are the non-applicability of certain social security laws of the receiving State and the exemption from civic duties.
- Facilities are typically courtesies extended by the receiving State to enable diplomatic missions and their agents to carry out their functions smoothly. Requirements, such as assisting the mission in finding suitable premises, facilitating free communications, and allowing free travel within the receiving State, are examples of facilities.

This section will first elaborate on State immunity, followed by the immunities of Heads of State and Government. It concludes with an analysis of immunities, privileges, and facilities of diplomatic and consular missions and staff.

4.1 State Immunity

Until the twentieth century, States enjoyed absolute immunity for any act; such an absolutist conception of sovereignty deprived individuals and corporate entities of any remedy when a public administration failed to honour its legal obligations under ordinary contracts. However, it gradually became accepted that whenever a State authority acted in the same way as a private person or entity (e.g. in commercial activities), it should not enjoy immunity. By the end of the nineteenth century, the concept of qualified immunity had been introduced in international law. During the twentieth century, qualified immunity gradually replaced absolute immunity, introducing the distinction between

acts *iure imperii,*[90] where the State exercises its sovereign power and *iure gestionis*, where the State behaves as if it were a private entity.[91, 92]

The question of sovereign immunity may appear in internet issues. If a State acts in order to protect its online facilities, it is done in an *iure imperii* capacity which provides a State with necessary immunity. Most other cyber activities will be considered *iure gestionis*, so a State will not be able to enjoy immunity.

4.2 Immunities of Heads of State and Government

The distinction between the immunity of States and that of Heads of State is a new development in international law. In the past, Heads of State had the same immunity as the State. In modern international law, these two types of immunities are different.[93]

No mention of Heads of State occurs in the VCDR. The UN *Convention on Special Missions* of 1969 mentions, in Article 21, that Heads of State enjoy 'privileges and immunities accorded by international law to Heads of State on an official visit', but it does not elaborate further.[94] However, it is widely accepted that international customary law grants privileges and immunities to Heads of State, a practice which originated during the times of absolute monarchies, when the sovereign enjoyed absolute immunity.[95] This approach is confirmed by international jurisprudence. In the *Congo* case, the ICJ reaffirmed the principle of immunity of a Head of State and other high officials. The Court stated: 'in international law it is firmly established that [...] certain holders of high-ranking offices, such as the head of State, head of government and minister of foreign affairs, enjoy immunities from jurisdiction in other states, both civil

90 An example of an act *iure imperii* is the use of the army in an armed conflict. In 1989, in the case of the Argentine Republic v. Amerada Hess Shipping Corporation, the United States Supreme Court found no difficulty in granting immunity to Argentina against a claim filed by the owner of a tanker that the Argentine Air Force had attacked and damaged on the high seas during the Falklands War.

91 The main problems of classification occur in the grey zones that come before the courts. A poignant example is the situation where States purchase military tanks. It is not always clear whether these transactions should be treated as cases of *iure imperii* (strengthening the armed forces) or as cases of *iure gestionis* (entering into commercial transactions). Two approaches have been used in determining the nature of State actors in this grey zone. First, an objective test may check the nature of a particular act, for example, to determine whether it is a commercial act. A second, subjective, test may be based on the purpose of a particular act. These two approaches are useful in solving many problems, but some issues remain open. For example, according to the objective test the purchase of army boots is considered *iure gestionis* (a commercial transaction). According to the subjective test, however, it could be an act *iure imperii* since army boots are purchased to perform one of a State's sovereign functions (defence).

92 See P. Malanczuk, *Akehurst's Modern Introduction to International Law* (London: Routledge, 1997), p.120.

93 It is also relevant that in certain countries, for example the United States, the Head of Government is also the Head of State, that is, the President. In some other countries, the position of Head of Government is separate from that of a largely ceremonial Head of State (in the United Kingdom, for example, the Head of State is the Queen).

94 *Convention on Special Missions*, 1400 U.N.T.S. 231.

95 See Malanczuk, *supra* note 92, p.119.

and criminal.'[96, 97] Immunities of Heads of State and Government should be analogous to diplomatic immunities and include immunity from criminal and civil jurisdiction; inviolability of residence, person, and movable property; freedom of communication, etc.

The alleged surveillance of the Presidents of Brazil, Mexico and others by the NSA could raise the question of a breach of international customary rules guaranteeing immunities for Heads of State.[98] Respective revelations triggered official diplomatic protests, the postponement of the visit of the Brazilian President to the US, and the first diplomatic actions in the UN system (discussion in the UN Security Council, address by the President of Brazil at the UN General Assembly).

4.3 Diplomatic Immunities, Privileges and Facilities

4.3.1 Inviolability of Hardware and Digital Assets

The immunities accorded to the mission premises are endorsed in Article 22(1) of the VCDR which States that the mission premises shall be inviolable. Denza elaborates on what the concept of inviolability entails: 'Inviolability in modern international law is a status accorded to premises, persons or property physically present in the territory of a sovereign state, but not subject to its jurisdiction in the ordinary way.'[99] Furthermore, according to Article 22(2) of the VCDR, the receiving State has a special duty to protect the mission from any intrusion or damage, and to prevent any disturbance of the peace of the mission, or the impairment of its dignity. In practice, receiving States have rigorously followed the principle of the inviolability of missions and any exceptions usually occur by accident or by mistake. Probably the most memorable recent event that illustrates the failure of a receiving State to protect the premises of a diplomatic mission took place between 4 November 1979 and 20 January 1981, when the militant university students seized the US Embassy in Tehran. The students later received support from the Khomeini regime. In its *Teheran Hostages* judgment, the ICJ specified that the 'Iranian government failed to take appropriate steps to protect the premises, staff, and archives of the United States mission against attack by the militants, and to take steps to prevent or stop the attack.'[100]

---

96 *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)*, Judgement, I.C.J Reports 2002, p. 21.

97 A. Cassese 'When may senior State officials be tried for international crimes? Some comments on the *Congo v. Belgium* case.' (2002) 13 *European Journal of International Law* 853–975.

98 Reuters, 'NSA spied on communications of Brazil and Mexico Presidents' *The Guardian US* (2 September 2013) <http://www.theguardian.com/world/2013/sep/02/nsa-spied-mexico-brazil-presidents> accessed 17 October 2013.

99 E. Denza, *Diplomatic law: Commentary on the Vienna Convention on Diplomatic Relations* (Oxford: Clarendon Press, 1998), p.112.

100 Teheran Hostage Case, *supra* note 42, para. 86.

Inviolability of diplomatic premises also extends to computers, printers, and other information technology facilities located on the mission premises. However, it is not clear whether inviolability could be extended to digital assets which are located outside the mission on, for example, internet servers in a cloud. For the protection of this type of digital asset, the closest analogy is the protection of bank accounts, which are held outside the premises of the mission. The VCDR did not regulate the status of such bank accounts – presenting circumstances which required additional interpretation of the Convention. Denza argues[101] that decisions of national courts and international practice confirm the international customary rule that inviolability can be extended to bank accounts if they are used for activities of diplomatic missions.[102] Article 25 of the CSM goes beyond the VCDR regulation and includes inviolability to 'other property used in the operation of the special mission'. Digital assets can enjoy the same protection as bank accounts. However, some digital assets such as electronic documents could enjoy wider protection via the provision of Article 24 of the VCDR that guarantees protection of diplomatic archives 'at any time and wherever they may be'. Even in the case of the closing of a diplomatic mission, diplomatic archives that include electronic documents will enjoy diplomatic immunity.

Consular posts do not enjoy as broad inviolability as diplomatic ones. Based on the Article 31 of the VCCR there are two major differences between the status of premises of diplomatic missions and those of consular missions. First, the inviolability of consular mission premises covers only those parts used for the work of the consulate, rather than the entire premises; second, and more importantly, consent to enter premises is assumed in the case of fire or other disasters.

It remains open to interpretation whether the right of the receiving State to enter consular premises in the case of 'fire and *other disasters*' (Article 31 of the VCCR, emphasis added) also covers a potential cyber disaster in the form of a major cyber attack and internet disruption. The provision of the right for emergency entry to consular premises was drafted in the view that most consular premises are located in the building with other tenants (unlike diplomatic missions which typically use villas or separate houses).[103] In the case of a fire on consular premises, other flats and offices could be endangered if there is not timely reaction by fire-fighters or other emergency services. One can argue that the same spirit that inspired the drafters of this provision (limited inviolability of consular premises in the case of disaster) could be used for dealing with cyber disasters when they create a risk for others. Digital facilities on consular premises could be used as a source of cyber attacks that could endanger the receiving State's internet system.

101 Denza, *supra* note 99, pp.133–134.

102 The inviolability of embassies' bank accounts was confirmed by the German Federal Constitutional Court in 1977 in the case: Philippine Embassy Bank Account. An Austrian court took a similar decision in the case Republic of 'A' Embassy Bank Account Case.

103 This practice has been changing. In the main diplomatic centres (e.g. Geneva, Brussels, New York) embassies and permanent missions are increasingly located in business buildings alongside business offices.

As it is the case with a 'botnet', this could be done without knowledge of the officials of the consular office.[104]

4.3.2 Freedom of Diplomatic Communication

One of the postulates of diplomatic law is that diplomatic missions are entitled to free communication: communication that is unmonitored, unobstructed and free from surveillance or interference. Since Article 27 of the VCDR specifies that 'the mission may employ all appropriate means' of communication, this should include the use of the internet.

Article 27 of the VCDR introduces a special responsibility for the receiving State to 'permit and protect free communication on the part of the mission for all official purposes'. However, the internet architecture may bring problems for the receiving State in its duty to protect a mission's communication from possible interference and surveillance. Most diplomatic missions connect to the internet via local internet service providers, allowing easier access to diplomatic communication to a wide range of actors, including intelligence services and malicious actors. One early example of the limited possibilities for a receiving State to protect internet communication was the publishing in a Turkish newspaper of an intercepted email sent by the European Union delegation in Turkey in 2002.[105] The European Union demanded that the Turkish government take measures to enhance the security of its diplomatic representation in Ankara, pointing out that the correspondence was protected under the Vienna Convention.

The Snowden revelations of the online surveillance by the NSA brought the question of protection of diplomatic communications into sharper focus. These include allegations of reports of the electronic surveillance of 38 embassies and missions in the US whose communication was intercepted by the NSA,[106] and of extensive surveillance of local electronic communication by embassies of the US, UK, Canada and Australia in Bangkok, Beijing, Jakarta, Hanoi and other Asians capitals.[107] Leaked documents also

---

104 'A botnet (also known as a zombie army) is a number of internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the internet. Any such computer is referred to as a zombie - in effect, a computer 'robot' or 'bot' that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets – not spam, viruses, or worms – currently pose the biggest threat to the internet. A report from Symantec came to a similar conclusion.' SearchSecurity, 'Definition botnet (zombie army)'. See <http://searchsecurity.techtarget.com/definition/botnet> accessed 18 October 2013.

105 C. Collins, 'EU envoy's e-mail riles many Turks' *Chicago Tribune* (27 February 2002) <http://articles.chicagotribune.com/2002-02-27/news/0202270288_1_mails-e-mails-turkish-media> accessed 09 November 2013.

106 E. MacAskill and J. Borger 'New NSA leaks show how the USA is bugging its European allies' *The Guardian* (30 June 2013) <http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies> accessed 17 October 2013.

107 For more information see: 'Australian ambassador summoned amid Asia US spying reports' BBC <http://www.bbc.co.uk/news/world-asia-24757968> accessed 09 November 2013.

indicate heavy surveillance of multilateral meetings. In 2009, the UK's Government Communications Headquarters – the British e-spying agency – reportedly monitored mobile and computer communication of world leaders and diplomats attending the G20 meeting in London.[108]

The Snowden revelations raise the question of whether the internet surveillance of diplomatic missions and diplomats is in accordance with international law and the national law of the host State, where the mission and diplomats are based. In international law, the VCDR is clear in stipulating that surveillance of diplomatic communication and access to diplomatic documents could be deemed a breach of Article 27 of the VCDR. Internet surveillance is also in breach of Article 24 of the VCDR: 'The archives and documents of the mission shall be inviolable at any time and wherever they may be.'[109] Besides the host State, Article 40(3) of the VCDR requires third-party countries to protect diplomatic communication in transit. It extends protection of diplomatic communication to all places where internet communication passes. For example, diplomatic messages going from a diplomat's computer in Geneva, to a server in the US should, according to the respective interpretation of the VCDR, enjoy protection along the internet route. In such a case, Article 40 of the VCDR forms the basis for the legal assessment of the legality of the interception of e-mail communication outside of the country where the diplomat is accredited.

While the VCDR provisions are clear in making surveillance of diplomatic missions and diplomats illegal, some authors open discussion of legality of surveillance based on the fact that it is widely practiced by many States. Simon Chesterman stresses the limits of the development of international customary rules that could provide legal justification for surveillance: 'if the vast majority of states both decry it and practice it, State practice and *opinio juris* appear to run in opposite directions'.[110] Some other authors try to develop a legal basis for surveillance of diplomats by stressing that surveillance must be done within customary normative limits.[111] Although the surveillance of diplomats is practiced by many countries, it is not possible to find arguments for considering it legal under international customary law for the following reasons: first, existing treaty law – the VCDR – prohibits the surveillance of diplomats and diplomatic missions; second, the VCDR is the codification of international customary law. Surveillance of diplomats cannot be considered to be a new custom developed since the adoption of the VCDR. Surveillance is as old as diplomacy and if the customary rules on the surveillance of

108 McAskill et. al., *supra* note 86.

109 See section 4.3.3.

110 S. Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 Michigan Journal of International Law, p. 1072.

111 S. M. McDougal, H. D. Lasswell, and W. M. Reismann, 'The Intelligence Function and World Public Order', (1973) 45 Temple Law Quarterly 365.

diplomats existed, they could have been considered back in the 1961 when the VCDR was adopted.

On the national level, the Snowden revelations have also positioned the topic of freedom of diplomatic communication within the debate on freedom of the press versus national security. The UK government requested *The Guardian* to stop publishing sensitive documents revealed by Snowden,[112] but did not initiate legal proceedings as it did in 1987 when a former British spy, Peter Wright, who moved to Australia, published the book *Spycatcher* explaining the communication surveillance of diplomatic missions in London. After *The Guardian* and *The Observer* started publishing his memoirs, the British government filed court proceedings requesting that the publication of the confidential documents to be stopped. The High Court accepted *The Guardian*'s arguments that it is in the public interest to expose surveillance of foreign missions as a breach of both international and British law.[113] The ruling of the British court was supported by the European Court of Justice.[114]

The legal obligation of a host State to restrain from surveillance of diplomatic communication is clearly stated by F. Seysterd:

> The receiving State must not attempt to become acquainted with the contents of the communications--and it must take all reasonable precautions to prevent others from doing so. Thus the receiving State does not have tile right to censor ordinary mail, or to open the diplomatic bag, or to listen in to telephones or private conversations, or to copy or decipher telegrams. *If it employs these practices in respect of its own citizens, it must make an exception for diplomatic communications*.[115]

4.3.3 Use of Wireless Facilities by Diplomatic Missions

Article 27(1) of the VCDR governs the right to use a wireless transmitter. It presents the main technology-related provision of the VCDR and was one of the most controversial aspects in the negotiation of the VCDR.[116] Technologically advanced countries argued for full freedom of the use of wireless communication by diplomatic missions.[117] Developing

---

112 The prime minister has called on the Guardian and other newspapers to show 'social responsibility' in the reporting of the leaked NSA files, to avoid high court injunctions or the use of D-notices to prevent the publication of information that could damage national security. For more information see <http://www.theguardian.com/world/2013/oct/28/david-cameron-nsa-threat-newspapers-guardian-snowden>.

113 BBC, 'Government loses Spycatcher battle' (13 October 1988) <http://news.bbc.co.uk/onthisday/hi/dates/stories/october/13/newsid_2532000/2532583.stm>.

114 European Court of Justice, *Case of Observer and Guardian v. the United Kingdom*, Judgement, 26 November 1991 <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57705>.

115 F. Seyersted 'Diplomatic Freedom of Communication' *Scandinavian Studies in Law* (Stockholm: Almqvist & Wiksell International 1970) 193, 209 [emphasis added].

116 Denza, *supra* note 99, 1998, p. 175

117 Amendment by United Kingdom: UN Doc. A/Conf. 20/C 1/L 291.

countries proposed a formulation which would require consent of the receiving State and observation of national laws and international telecommunication regulations.[118] At that time, wireless communication related mainly to radio transmission. In arguing for restricted wireless communication, developing countries maintained that they needed the right to grant permission in order to implement the provisions of Article 6 of the *Constitution of the International Telecommunication Union* which specifies that the State has responsibility to ensure that any telecommunication originating from its territory does not cause 'harmful interference to the radio services of other countries.'[119] In Article 48, the ITU Constitution mentions only military radio installations as exceptions which do not require application of the ITU Constitution.[120] On this basis, developing countries argued that the ITU Constitution applies to diplomatic wireless facilities since they are not mentioned as an exception in the ITU Constitution. This argument prevailed in the negotiations and Article 27(1) of the VCDR specifies that '[…] the mission may install and use a wireless transmitter only with the consent of the receiving State.' There are two possible consequences of this stipulation for internet communication.

The first is related to the use of wireless facilities in diplomatic missions for the electronic surveillance of local communication in the capital of the host country, as it is reported to be done by the US, the UK, Australia and Canada in the capitals of Asian countries.[121] The Chinese MFA reacted to this allegation by requesting that 'foreign embassies in China and their staff respect the Vienna Convention.'[122] There are two potential breaches of the VCDR: of Article 27(1), stating that a wireless transmitter should be used only for the communication of diplomatic missions; and of Article 41 (1) and (3), endorsing the duty of the diplomatic mission to observe local law. As a first reaction, the affected countries might issue a diplomatic protest note. The next step may require a mix of legal and technical measures that should prevent future electronic surveillance (e.g. assurances, including possible inspection, that the embassies' equipment is used only for wireless communication with the capital). The possibility of more radical measures was indicated by Bhagevatula Satyanarayana Murty: 'If electronic surveillance seriously threatens the security of the receiving State, it is likely to demand the closure of the mission.'[123]

The second likely consequence is related to the rapid development of new wireless technologies which may provide diplomatic missions with new types of wireless

118 Amendment by India on behalf of 14 developing countries: UN Doc. A/Conf. 20/C 1/L 165.

119 Article 2 of the *Constitution of the International Telecommunication Union*.

120 *Ibid*, Article 48.

121 For more information see 'Australian ambassador summoned amid Asia US spying reports' BBC (1 November 2013) <http://www.bbc.co.uk/news/world-asia-24757968> accessed 09 November 2013.

122 *Ibid*.

123 B.S. Murty, *The International Law of Diplomacy: The Diplomatic Instrument and World Public Order* (Martinus Nijhoff 1989) p.506.

communication. These would require the permission of host countries for their use, even if they become more like digital commodities than like the complex technical facilities they were back in the 1960s when the VCDR was drafted. Additionally, giving international telecommunication regulations priority over diplomatic law (as was done in the negotiation of Article 27(1) of the VCDR) may be used in the future by States to reduce the freedom of diplomatic communication on the basis of enforcing telecommunication standards and regulations.

4.3.4 Inviolability of Databases and Electronic Documents

Preparing and managing diplomatic documents has been substantially affected by the internet. Diplomats draft documents using word processors and store them on hard disks or servers in a cloud. Diplomatic documents are transmitted over the internet. A lot of negotiation is done by drafting diplomatic documents with the use of track changes and annotations.

It is only a few decades since documents were produced by a much slower process, starting with hand-writing the first draft, typing the official version, and storing it in the archive. This is, for example, how documents were prepared when negotiators were drafting the VCDR. In spite of major changes in technology, however, the VCDR's provisions on the protection of diplomatic documents are still appropriate in the internet era.

Archives and documents, including electronic ones, enjoy the strongest protection by the VCDR, which states in Article 24 that '[t]he archives and documents of the mission shall be inviolable at any time and wherever they may be.' Even in the case when a mission premises loses its diplomatic status due to a severance of diplomatic relations, the archives and documents retain their inviolability without a time limitation. Such high protection was inspired by the importance of confidentiality with regard to the work of diplomatic services. The initial draft of Article 24, which referred only to 'archives', was amended by adding 'documents' in order to also cover less formal documents that do not form part of official archives, such as negotiating drafts, 'non papers' and memoranda in draft.[124] This wide interpretation of the concept of an archive was restated by the International Law Commission in its work on the *Convention on the Succession of States*, where an archive is defined as 'documentary material of whatever kind amassed and deliberately preserved by State institutions in the course of their activities'. The phrase 'of whatever kind' includes electronic documents and e-mail.

Additional protection for archives and documents is provided by Article 30 of the VCDR that extends the inviolability to correspondence and papers, even those that may

[124] The VCCR provides more precise definition of archives in Article 1(1): '[…] all papers, documents, correspondence, books, films, tapes and registers of the consular posts, together with the ciphers and codes, the card-indexes and any article of furniture intended for their protection or safe-keeping.'

be private. One justification for including all correspondence and papers into the scope of the provision was to reduce the temptation of a receiving State to search papers and classify them as private or official.

If strictly applied, the provisions of the VCDR provide diplomats with a wide protection of their documents. The wording of Article 24, protecting diplomatic archives and documents 'wherever they may be' also includes databases, electronic documents and emails stored in cloud servers and services such as GoogleDocs. The application of the existing VCDR regulations creates some practical challenges.

First, in order to provide necessary protection, internet companies would need to identify documents and messages as diplomatic ones (e.g. documents on GoogleDocs or messages on gmail servers). The VCDR, including *traveaux préparatoires*, does not provide useful solutions for the identification of diplomatic digital assets. During the negotiations of the VCDR, France and Italy proposed an amendment requiring that diplomatic documents outside the premises of the mission 'must be identified by visible official signs.'[125] The proposal was not accepted. Thus, diplomatic archives and documents found outside the mission enjoy immunity, even if they are not clearly marked or otherwise identifiable as diplomatic documents. This decision does not help to solve the question of the immunity of diplomatic digital assets saved on servers in a cloud. Most likely, a new rule will develop either through 'instant customary law' or explicit regulation, requiring some type of digital identification of diplomatic archives and documents (e.g. special registration, using dedicated diplomatic servers).

Second, questions arise with regard to the universality of diplomatic immunities. According to Article 24 of the VCDR 'the archives and documents of the mission shall be inviolable at any time and wherever they may be'. 'Wherever they may be' makes diplomatic privileges very virtual, and opens a potential responsibility for any government, including beyond the receiving country where the diplomat is based, to protect digital documents stored on cloud servers or in transit over a network under their jurisdiction. In 1961, when the VCDR was drafted, physical limitations to the movement of documents and archives existed: they had to be typed up and distributed. Since these physical limitations no longer exist, the principle of universality of diplomatic protection may need to be re-examined and, possibly, limited.[126]

Thirdly, the question arises as to what governments can do to ensure immunity for electronic documents and archives. In international law, legal action based on diplomatic or consular immunities cannot be taken against private companies, for example, Google or Facebook, which may be involved in the breach of e-immunity. Obligations in

125 UN Doc. A/Conf. 20/C 1/L 149 (Amendment of France and Italy); A/Conf. 20/14, p. 49.

126 J. Kurbalija, 'Do e-mail and e-documents have diplomatic protection?' *Diplo* (Geneva, 13 June 2013) <http://www.diplomacy.edu/blog/do-e-mail-and-e-documents-have-diplomatic-protection> accessed 09 November 2013.

international law exist between States. National governments have a responsibility to ensure that individuals and institutions under their jurisdiction comply with international law, namely the VCDR. Thus would, for example, the US government be responsible for ensuring that any email of any diplomat, stored on, for example, a gmail server, be protected according to diplomatic immunity rules? The search for the answer to this question should start with Article 29 of the VCDR which states that governments must take 'all appropriate steps' to ensure the protection of diplomats. The VCDR *traveaux préparatoires* can help in the interpretation of the phrase 'all appropriate steps'. Belgium proposed the formulation that receiving States should take 'all steps' in order to ensure protection of diplomatic missions and diplomats.[127] In challenging the Belgian proposal, the UK representative suggested that the formulation 'all steps' would 'impose an impossible task on receiving state'.[128] Respecting the spirit of the way Article 29 of the VCDR was drafted, 'all appropriate steps' for protection of diplomatic digital assets should involve steps that could be technically implemented by the receiving State. An important pre-condition will be to provide a way to identify diplomatic digital assets, in order to help internet companies provide the diplomatic protection specified by the VCDR. National governments should also ensure responsibility for natural and legal entities under their jurisdictions, including internet companies, in the case of a violation of the immunity of diplomatic digital assets.

4.3.5 Exemption from Custom Duties for E-Purchase

Article 36 of the VCDR deals with exemption from customs duties and inspection. It states that articles intended for the use of the diplomatic mission and for the personal use of a diplomatic agent (or members of their family) are exempt from all customs duties, taxes, and related charges. This exemption does not apply to charges for carriage, storage, and similar services. Furthermore, according to Denza, Article 36 puts the receiving State under an obligation to permit entry of those articles intended for diplomatic use.[129] This regulation applies to online purchases as well. However, an online purchase faces the same limitations as a regular purchase of objects that are prohibited under the domestic law of receiving State (e.g. certain online materials). In such cases, Article 41 of the VCDR applies, stating (and being the overruling obligation) that a diplomat has to respect the laws and regulations of the receiving State.

5. The Future of Diplomacy and Diplomatic Law in the Internet Era

This chapter addressed the question whether the internet has triggers 'just another evolutionary step' in the long history of diplomacy, or actual revolutionary changes in

127 UN Doc. A/Conf. 20/C 1/L 214.

128 A/Conf. 20/14, p. 160.

129 Denza, *supra* note 99.

the way how, where and by whom diplomacy is performed. Some diplomatic functions, such as information gathering, already have been profoundly affected by the internet. Others, such as representation and negotiation, have been less affected. The internet has also started to affect the three core elements of the organisation of diplomacy and its professional culture: hierarchy, exclusivity, and secrecy. Diplomatic services are organised hierarchically, according to rank, starting from attachés and ending with ambassadors. Internet tools – based on sharing of, and easy access to, information – are increasingly challenging hierarchical work processes in diplomatic services. Exclusivity is one of the characteristics of diplomacy that can be traced back to its aristocratic origins. This feature of diplomacy could create tensions with the more open, and less formal, social ethos fostered by internet communication. The most profound and visible impact of the internet is on the secrecy of diplomatic services. The WikiLeaks release of diplomatic cables and recent Snowden revelation are the most visible examples of the need to maintain secrecy.

With regard to diplomatic law, in spite of the major technological changes over the last five decades, the 1961 VCDR, the core instrument of diplomatic law, has survived the test of time. It is one of the most observed international legal instruments. The main, internet-driven, challenges to the VCDR will be related to the provisions on information gathering and communication.

When the VCDR was drafted, information gathering and communication were two separate activities. Information was gathered, analysed, and stored in the MFA's archives. Communication was conducted in person and principally through the use of telephone and telegraph. This is why these functions are regulated separately in Article 23 (information, i.e. archives and documentation) and in Article 27 (communication, i.e. official correspondence). Today, an interplay and overlap between communication and information can be identified. By storing data on a server in a cloud, both communication (i.e. transmitting data over the internet) and saving it in a digital archive (namely in servers in a cloud) are interlinked. Ideally, a possible new provision would regulate in an integrated way both the communication and information aspects of digital activities.

The internet has also introduced new forms of communication among diplomats, as well as between diplomats and the public. For example, Twitter has become a usual practical tool in diplomatic activities. By using Twitter and the internet in general to communicate with institutions, individuals and receiving States, diplomats could be in breach of Article 41(2) of the VCDR which states: 'All official business with the receiving State entrusted to the mission by the sending State shall be conducted with or through the Ministry of Foreign Affairs of the receiving State or such other ministry as may be agreed.'

This provision is the one which could be deemed most obsolete. It was already superseded in the pre-internet era by diplomats communicating more directly with institutions and individuals in the receiving State.

Despite frequent requests to amend the VCDR, not only due to technological developments, but also to abuse of privileges and immunities, it is difficult to envision major changes to the treaty. The VCDR is ratified by nearly all States and is, in general, observed. It is one of the pillars of international law. The most likely scenario is that the VCDR will be adapted to internet-driven changes through a modern interpretation of the existing provisions. Another possible development might be the adoption of an 'internet protocol' augmenting the VCDR, which would provide both clarification of the use of existing rules in the internet arena and provisions for regulating new, internet-related issues, such as virtual representation or the immunities of diplomatic documents stored in a digital cloud.

*Katharina Ziolkowski**

Peacetime Cyber Espionage – New Tendencies in Public International Law

1. Introduction

Espionage has existed since the dawn of human history. The earliest record of espionage dates from the times of Pharaoh Ramses (ca. 1274 BC).[1] One of the oldest cases of economically motivated espionage – on a scale affecting national interests – might be the legend of a Chinese princess who, in about 440 AD, when married to a foreign ruler, smuggled silk worms – by then a national secret of silk production – out of the country, hiding them in her hair (admittedly, artfully attired and rather big those days).[2] History offers countless other examples of politically or economically motivated intelligence gathering by foreign States.[3]

With the development of the internet into a global 'network of networks' times changed significantly and heralded a 'golden age' of espionage. Cyber espionage reduces risks to intelligence agencies (e.g., with regard to 'turned' spies) and their personnel (to be caught), allows large-scale out-sourcing[4] of intelligence collecting activities, and offers possibilities hitherto unheard of in terms of the ease, swiftness and inexpensiveness of intelligence gathering and with regard to the amount of information to be collected. Today's 'Internet of Things' includes approximately 12.5 billion[5] devices connected to the global net, and is predicted to evolve in the next five to ten years into the 'Internet of

* Due to limited research resources, the assessment of secondary legal sources is primarily based on scholarly writings available online. The author is deeply indebted to the NATO ACT - SEE Legal Office for providing access to various online databases.

1 cf Terry Crowdy, *The Enemy Within. A History of Espionage* (Osprey 2006) 15; *Gale* Encyclopedia of Espionage *& Intelligence*, 'Espionage and Intelligence, Early Historical Foundations' <http://www.answers.com/topic/espionage-and-intelligence-early-historical-foundations>.

2 Karen Sepura, 'Economic Espionage: The Front Line of a New World Economic War' (1998-1999) 26 *Syracuse Journal of International Law and Commerce* 127, 129 (with further references), Susan W Brenner and Anthony C Crescenzi, 'State-Sponsored Crime: The Futility of the Economic Espionage Act' (2006) 28 *Houston Journal of International Law* 389, 395 (with further references). See also 'History of Silk' <http://www.silk-road.com/artl/silkhistory.shtml>.

3 eg the secret of producing high-quality China bone porcelain, poison gas (first used during World War I as a weapon) or bidding price information with regard to contracts bids, intercepted by strategically deployed 'flight attendants' on international flights, see Sepura (n 2) 130f and, Brenner and Crescenzi (n 2) 395 (with further references).

4 cf WikiLeaks, 'Spyfiles' <http://wikileaks.org/spyfiles3.html> (containing 249 documents from 92 global intelligence contractors).

5 Estimation as of 2010, cf Dave Evans, 'The Internet of Things. How the Next Evolution of the Internet is Changing Everything' (*CISCO IBSG White Paper*, April 2011) <http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>.

Everything', with possibly 30 billion[6] devices connected wirelessly. Thus, a significant growth of the domain for harvesting by intelligence agencies is to be expected in future.[7]

Recently, cyber espionage received a lot of attention, not only due to publicly available information about major espionage operations like *GhostNet,*[8] *Shady RAT,*[9] *Flame,*[10] and the highly sophisticated, persistent and still active *Red October*,[11] of which the operators are yet unknown, but also due to the recent revelations about the alleged mass surveillance programmes of the Unites States (US), code-named 'PRISM' and 'Boundless informant',[12] involving cooperation with giant market leaders like Microsoft, Apple, Google, Facebook, Yahoo, YouTube, Skype, AOL, and PalTalk, [13] as

6 eg Allied Business Intelligence (ABI), 'More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020' (*ABI research news*, 9 May 2013). <https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne>.

7 As a superior of the author rightly pointed out, there 'will be no secrets stored in a ["cybered"] refrigerator'. However, surveillance, especially if a refrigerator is wirelessly connected to a supermarket's shopping list, can provide information about the weekly schedule, social events planned, behavioural patterns or, more generally, the mood of the 'person of interest'.

8 The *GhostNet* operation was discovered in 2009 and is said to have successfully infiltrated computer systems of embassies, foreign ministries, and other government offices in 103 countries, including the Dalai Lama's Tibetan exile centers in India, London and New York City. The SecDev Group, 'Tracking GhostNet: Investigating a Cyber Espionage Network' (Infowar Monitor Report, 29 March 2009) <http://de.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>.

9 Between 2005 and 2011 this Remote Access Tool (RAT) targeted over 70 global companies, governments and non-profit organisations. See Dimitri Alperovitch, 'Revealed: Operation Shady RAT' (White Paper, McAfee 2011) <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.

10 *Flame* was active between 2010 and 2012; after the public exposure the malware received from its 'masters' a 'kill command' and wiped all its traces form the infected computers. *Flame* targeted government organizations, educational institutions and private individuals in Israel, Palestine, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt, and especially in Iran. See Damien McElroy and Christopher Williams, 'Flame: World's Most Complex Computer Virus Exposed' *The Daily Telegraph* (28 May 2012) <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html>.

11 *Red October* targeted, among others, governmental (including diplomatic), communication as well as the nuclear and energy (including oil and gas), military and aerospace sectors. See Kaspersky, '"Red October" Diplomatic Cyber Attacks Investigation' (Report, 14 January 2013) <http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation>; Pierluigi Paganini, 'Operation Red October : Cyber Espionage campaign against many Governments' *The Hacker News* (14 January 2013) <http://thehackernews.com/2013/01/operation-red-october-cyber-espionage.html#ixzz2jfYuhWh3>. The command and control structure of *Red October* is extremely complex and extended, so even a mere speculation in regard to the technical attribution to a State's territory is impossible.

12 cf Glenn Greenwald and Ewen MacAskill, 'Boundless Informant: the NSA's secret tool to track global surveillance data' *The Guardian* (11 June 2013) <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>; Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program' *The Washington Post* (7 June 2013) <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

13 eg Ed Pilkington, 'Washington Post releases four new slides from NSA's Prism presentation' *The Guardian* (30 June 2013) <http://www.guardian.co.uk/world/2013/jun/30/washington-post-new-slides-prism>; Ellen Nakashima, 'Verizon providing all call records to U.S. under court order' *The Washington Post* (6 June 2013) <http://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_story.html >.

well as a classified programme code-named 'Bull-run',[14] allegedly allowing the US to circumvent or crack much of the encryption that guards global commerce and banking systems. Indeed, hacking by intelligence agencies or their proxies offers a multitude of interesting topics, such as the cooperation with or use of the highly talented criminal underworld and their tools (e.g., botnets – millions of hijacked 'zombie' computers belonging to innocent individuals)[15] or the procurement of information on vulnerabilities (especially hitherto unknown 'zero-day' vulnerabilities) and other 'entry vectors' into information technology (IT) systems and computer programmes, as well as of 'exploits' from highly specialised private companies such as the Malta-based 'Revuln' or France-based 'Vupen',[16] amongst others. Although governed by national intelligence laws and supervised, the intelligence community has always formed – in a way and for good reasons – a separate world that is not easily known by outsiders. However, in combination with hacking, its technical sophistication, the over 60 different 'Trojan families'[17] (including Remote Access Tools and 'backdoors' used) and 'techie'-language, it has definitely created another 'universe' that would be interesting to explore further.

This chapter focuses on the public international law assessment of peacetime espionage conducted by States, especially the shift in perception of cyber espionage as it is relevant to the national security of target States, and the proposals offered by some legal commentators to classify peacetime cyber espionage as 'threat' or 'use of [armed] force' and as 'armed attack' (the latter justifying self-defence measures on the part of the State spied on) as well as judging 'cyber intrusions' into IT-systems or computer networks as a violation of the territorial sovereignty of the State on which territory or area under exclusive jurisdiction the respective systems and networks are physically located. These opinions will be further assessed in the context of international law policy considerations, centring in particular the questions of preserving the *status quo* of the distribution of conventional (i.e., economic and military) power of the post-industrial, developed States as opposed to the global distribution of asymmetric cyber power. The author advocates, *inter alia*, to distinguish questions of national security, armed attack and self-defence from the 'theft' of intellectual property by cyber means, of which the latter should be countered on the one hand by the remedies public international law currently offers victim States during peacetime and on the other hand by the enhancement of the cyber security and resilience of the own IT-systems and computer networks.

14 Nicole Perlroth, Jeff Larson and Scott Shane, 'N.S.A. foils encryption protection around globe' *International Harald Tribune* (7-8 September 2013) 1.

15 Botnets are usually used for distributed denial of service (DDoS) attacks, but can be rented (for small amounts of money) by hour, in order to be scanned, for instance, for computers of politicians and their family members.

16 'Governments are Big Buyers of Zero-Day Flaws' *InfoSecurity News* (15 July 2013) <http://www.infosecurity-us.com/view/33441/governments-are-big-buyers-of-zeroday-flaws/>.

17 Alex Cox, 'The Cyber Espionage Blueprint: Understanding Commonalities in Targeted Malware Campaigns' (RSA First Watch, Intelligence Report, 2013) 3.

To define peacetime cyber espionage for the purpose of a public international law assessment is not an easy task. Neither the rather general definitions of espionage as offered by encyclopaedias and dictionaries,[18] nor national (peacetime) law definitions (showing a different angle of perspective justified by focus on establishing individual criminal liability)[19] can be used as a basis to which the prefix 'cyber' could simply be added. All the various definitions of espionage as proposed – including those by a multitude of scholarly writers – show, however, some common aspects: espionage must be conducted clandestinely or under false pretences or disguise; by a State organ or agent, or be otherwise attributable to a State; and must target information not publicly available. Before merely 'cyberising' such a statement, a glance on specific 'cyber espionage' definitions seems useful. NATO does not have a definition of cyber espionage, but defines a similar concept, namely Computer Network Exploitation (CNE), as an '[a]ction taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage'[20] or as an action supporting Information Operations by the 'ability to get information about computers and computer networks, by gaining access to information hosted on those and the ability of make use of the information and the computers/computer networks'.[21] Neither definition shows the necessary level of specification required for a legal assessment. A rather good example of a cyber espionage definition can be found in the US Presidential Policy Directive on 'U.S. Cyber Operations Policy'[22] which defines cyber espionage as '[o]perations and related programs or activities conducted [...] in or through cyberspace, for the primary purpose of collecting intelligence [...] from computers, information or communication systems, or networks with the intent to remain undetected. [...].' However, neither is this definition exact enough to be useful for an international law assessment, as it includes not only the espionage activity, but also activities merely adjunct to espionage, such as

18 Encyclopaedia Britannica defines espionage as 'process of obtaining military, political, commercial, or other secret information by means of spies, secret agents, or illegal monitoring devices. Espionage is sometimes distinguished from the broader category of intelligence gathering by its aggressive nature and its illegality', see *Encyclopædia Britannica*, 'Espionage' (online version) <http://www.britannica.com>; *Black's Law Dictionary* defines espionage as '[t]he practice of using spies to collect information about what another government or company is doing or plans to do', see Brian A Garner (ed), *Black's Law Dictionary* (7th ed, West Group 1999) 565.

19 Most of the national espionage definitions require the aspect of benefit to a foreign government, a foreign instrumentality or foreign agent, in order to draw a line between individual penal responsibility *versus* socially accepted information exchange in daily inter-human relations. See eg US Economic Espionage Act of 1996, 18 U.S.C. § 1831.

20 NATO, NATO Standardization Agency (NSA), *NATO Glossary of Terms and Definitions* (AAP-6 of 2013) 2-C-11 <http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf>.

21 NATO, *Allied Joint Doctrine for Information Operations* (Allied Joint Publication AJP-3.10, NATO/PfP UNCLASSIFIED, November 2009) 1-11 <http://info.publicintelligence.net/NATO-IO.pdf>.

22 The President of the United States of America, *Presidential Policy Directive/PPD-20* (TOP SECRET/NOFOR), U.S. Cyber Operations Policy, 2ff [available on WikiLeaks].

gaining of access[23] (comparable, in general terms, with 'entering a foreign territory' by a spy, before he or she conducts the actual espionage activity).

Therefore, for the purposes of the present chapter – and in recognition of the risk of incompleteness inherent in a detailed description – the following definition of cyber espionage is proposed:

> Cyber espionage is the copying of data that is publicly not available and which is in wireless transmission, saved or temporarily available on IT-systems or computer networks located on the territory or area under the exclusive jurisdiction of another State by a State organ, agent, or otherwise attributable to a State, conducted secretly, under disguise or false pretences, and without the (presumed) consent or approval of the owners or operators of the targeted IT-systems or computer networks or of the territorial State. Copying includes also the temporary copying of data into the random access or virtual memory of an IT-system for the purpose of mere visualization or acoustic exemplification of (e.g., voice over IP) data. The copying of data saved or temporarily available on IT-systems or computer networks located on the territory or area under exclusive jurisdiction of the copying State is covered by this definition only if the data is protected under public international law.

By focusing on the 'copying' of data, the definition emphasises that in cases of cyber espionage neither the integrity nor the availability of information contained therein is affected, but merely its confidentiality. This aspect is especially important in the context of a legal assessment, as the loss of confidentiality of data or information does not directly result in (physical) damage. The definition does not refer to the (e.g., political or purely economic) motivation of the spying State or to the level of importance of the information gathered for the targeted or spying State, in order to exclude aspects of subjectivity. It excludes extraction of data by bending fibre optic undersea cables, which would probably be classified as espionage, but is conducted by use of physical force, and not by 'hacking' an IT-system or computer network. The definition also excludes electronic reconnaissance and surveillance methods, sometimes referred to as 'national technical means' by arms control treaties, using, for example, satellites, long-range cameras and acoustic devices, as such methods do not include copying of data from IT-systems or computer networks. Not covered by the definition of 'cyber espionage' are activities merely adjunct to espionage. Those are all kinds of preparation activities such as obtaining access to IT-systems or computer networks, either remotely or by close access, modification of data in order to cover the intrusion, and potential activities that could follow espionage (such as subsequent transmission of previously saved data

23 ibid ('[...] Cyber collection entails accessing a computer, information system or network without authorization from the owner or operator of that computer, information system, or network or from a party to a communication or by exceeding authorized access. Cyber collection includes those activities essential and inherent to enabling cyber collection, such as inhibiting detection or attribution, even if they create cyber effects.').

to another individual or entity, data analysis, malicious computer manipulations) or accompanying conventional activities which are conducted covertly, though not online (on the US-specific aspect of 'covert action' or 'preparation of the battlefield' see section 2.1).

Importantly, this definition does not cover all cases of copying of data which has been saved (e.g., in a 'cloud') or temporarily available (e.g., transiting internet routers or so-called 'internet exchange points', IXPs) on servers located on the copying State's own territory or area under exclusive jurisdiction. In this context, IXPs are of particular importance. These are major data traffic knots in a particular geographical region, through which transit huge amounts of data following an automated 'traffic route decision' made by an internet router, but also possibly because of manipulation intended to direct data through a specific IXP. Although a trans-border aspect is present, the interception of such transiting data, or copying data saved on servers (for example, in a 'cloud') in the spying State's sovereign area, would be subject to national laws of the State in question, and to public international law only in the specific cases when the data is specifically protected by international law, e.g. due to its diplomatic nature (see section 2.3. for a detailed discussion). Only then does international law come into play, which is the sole subject of the present legal assessment.

There are two caveats. First, the legal assessment offered will cover only cyber espionage conducted by States, omitting espionage conducted by, for example, international organisations (as this volume focuses on State activities); however, the attribution of 'hackers' to a State, and thus questions of State responsibility, will not be addressed as it would exceed the scope of this chapter. Second, although 'intelligence gathering' is a concept much broader that 'espionage' – including, for example, open source information gathering – the two terms will be used interchangeably, however, for reasons of style and readability only.

2. International Law *de lege lata*

With regard to the legal assessment of peacetime espionage, different opinions are offered within legal writings. Some commentators assert that espionage is illegal.[24] Others claim that it is lawful.[25] The majority hold that peacetime espionage is neither

24 Ingrid Delupis, 'Foreign Warships and Immunity for Espionage' (1984) 78 American Journal of International Law 67; Manuel R Garcia-Mora, 'Treason, Sedition and Espionage as Political Offences Under the Law of Extradition' (1964) 26 University of Pittsburgh Law Review 79-80; Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' in Roland J Stanger (ed), *Essays on Espionage and International Law* (Ohio State University Press 1962) 12; Richard A Falk, 'Space Espionage and World Order: A Consideration of the Samos-Midas Program' in Stanger (ibid) 57.

25 Jeffrey H Smith, 'Keynote Address' (2007) 28 Michigan Journal of International Law 544; Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2007) 28 Michigan Journal of International Law 628, 636; Christopher D Baker, 'Tolerance of International Espionage: A Functional Approach' (2003-2004) 19 American University International Law Review 1092, 1094; John Kish, *International*

legal nor illegal.[26] Importantly, it must be noted that the examination of the (il)legality of espionage activities *per se* needs to be distinguished from the assessment of the (il)legality of actions adjunct to espionage, such as the unauthorised entrance into the sovereign territory of a State by a foreign agent.

2.1 Illegality of Espionage

The suggestions that espionage is illegal are partly[27] – and without further deliberations – based on the fact that espionage is penalised within domestic law systems. The argument is founded upon the perception that '[u]nder international law, if something were truly legal (or at least not illegal), no state should prosecute those who do it.'[28] This view does not fully appreciate the basic concept of sources of international law, especially of the 'principles of law recognized by civilized[29] nations' pursuant to Article 38(1)(c) of the *Statute of the International Court of Justice* of 1945 (ICJ Statute). This is the specific source of international law that elevates national law principles common to all domestic law systems to the level of international law, but only insofar as they are applicable to inter-State relations.[30] The general principles are identified by a method of successive

Law and Espionage (ed by David Turns, Martinus Nijhoff Publishers 1995) XV; Myres S McDougal, Harold D Lasswell and W Michael Reisman, 'The Intelligence Function and World Public Order' (1973) 46 Temple Law Quarterly (3) 395.

26 Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 Journal of National Security Law and Policy 195, 204ff; Luke Pelican, 'Peacetime Cyber-Espionage: A Dangerous Bur Necessary Game' (2010-2011) 20 CommLaw Conspectus 370; Robert D Williams, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2010-2011) 79 George Washington Law Review 1164, 1175; Major Arie J Schaap, 'Cyber Warfare Operations: Development and Use under International Law' (2009) 64 Air Force Law Review 121, 140; GN Barrie, 'Spying – An International Law Perspective' (2008) 9 Journal of South African Law / Tydskrif vir die Suid-Afrikaanse Reg (2) 238, 253; Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Michigan Journal of International Law 688; A. John Radsan, 'The Unresolved Equation of Espionage and International Law' (2006-2007) 28 Michigan Journal of International Law 596, 602 and 604; Baker (n 25) 1091f and 1094; Commander Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 Air Force Law Review 218, 223 (however, remarking at p 218 that espionage 'does not violate a principle of *jus cogens*' which does not correspond with the usual understanding of the sources of international law); Todd A Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 Case Western Reserve Journal of International Law 567, 580; Lt Col Geoffrey B Demarest, 'Espionage in International Law' (1996) 24 Denver Journal of International Law and Policy 321, 341 and 347; Leslie S Edmondson, 'Espionage in Transnational Law' (1972) 5 Vanderbilt Journal of Transnational Law (2) 444ff.

27 Garcia-Mora (n 24) 80, Radsan (n 26) 604.

28 Radsan (n 26) 604.

29 The reference to 'civilised' nations was included in Article 38 of the *Statute of the Permanent Court of Justice* (League of Nations) of 13 December 1920 (and was reproduced in the *Statute of the International Court of Justice*). During these times of euro-centric international law understanding, it was meant to exclude the rather 'primitive' law systems; nowadays, it does not have any discriminatory meaning, cf Wolff Heintschel von Heinegg, 'Die weiteren Quellen des Völkerrechts' in Knut Ipsen (ed), *Völkerrecht* (6th edn, CH Beck 2010) § 17 MN 2. However, Bassiouni claims that the expression still has utility when a given nation, because of peculiar historical circumstances, no longer follows its previously 'civilised' system of law, or that of the other 'civilised nations'. cf Mahamoud Cherif Bassiouni, 'A Functional Approach to General Principles of International Law' (1990) 11 Michigan Journal of International Law 768.

30 James Crawford, *Brownlie's Principles of Public International Law* (8th edn, Oxford University Press 2012) 34ff (with further references on the different opinions); Heintschel von Heinegg (n 29) § 17 MN 1; Brian D.

inductive accretions based on a comparison of the principal systems of domestic law.[31] Espionage activities are penalised within all principal systems of domestic law, of which a comparative analysis would certainly exceed the scope of this chapter.[32] However, the respective regulations govern *individual criminal liability* for espionage activities, which, for the specificity of the regulation (from which a principle would need to be derived) cannot be deemed a 'principle' of domestic law (such principles are,[33] e.g., responsibility and reparation for damages, unjust enrichment, property and indemnity). Additionally, one could assert that, due to the fact that matters of inter-State *political* relations are located at the level of international relations and not that of municipal law, a general principle with regard to inter-State espionage cannot be derived from the level of national law systems.

Another argument offered in favour of the illegality of espionage is the assertion that it violates the 'territorial integrity and political independence of other States'.[34] This view refers to the wording of Article 2(4) of the *Charter of the United Nations* (UN Charter), namely the prohibition of the 'use of [armed] force' in international relations, and confuses the 'collateriality' of physical intrusion of spying State aircraft, vessels, submarines or agents ('trespass') into the target State's territory with the act of espionage *per se*. Additionally, this opinion ignores that the above passage was introduced into the wording of Article 2(4) UN Charter upon insistence of some States which wished to underline the protection of the 'territorial integrity and political independence' against the 'use of [armed] force',[35] and the passage neither presents a prohibition itself nor indicates what would constitute 'use of [armed] force' which would affect that independence.

Espionage is asserted by one writer to be illegal under international law, even if not involving 'trespass', because it would 'offend[s] the principle of peaceful cooperation

Lepard, *Customary International Law. An New Theory with Practical Implications* (Cambridge University Press 2010) 164. For a discussion of the methodology see Stephen C. Hicks, 'International Order and Article 38(1)(c) of the statute of the International Court of Justice' (1978) 2 Suffolk Transnational Law Journal (1) 1-42. Petersen considers also 'general principles of international law' as covered by the norm (by analogy), see Niels Petersen, 'Customary Law Without Custom? Rules, Principles, and the Role of State Practice in International Norm Creation' (2008) 23 American University International Law Review 308.

31 Similarly Crawford (n 30) 35 (stating that tribunals have adopted modes of general reasoning as well as comparative law analogies); Robert Kolb, 'Principles as Sources of International Law (With Special Reference to Good Faith)' (2006) 53 Netherlands International Law Review (1) 10; Alain Pellet, 'Art. 38' in Andreas Zimmermann et al (eds), *The Statute of the International Court of Justice. A Commentary* (Oxford University Press 2006) MN 258; Wolfgang Friedmann, 'The Uses of "General Principles" in the Development of International Law' (1963) 57 American Journal of International Law 279, 282. For a discussion of the methodology see Hicks (n 30); Bassiouni (n 29) 788-792 (with examples of ICJ jurisprudence).

32 See eg for the common law system 18 USC § 1831-1839, for the civil law system § 94-99 of the German Penal Code, for the Sino-Asian law system Articles 110-111 of the Chinese Criminal Law.

33 Heintschel von Heinegg (n 29) § 17 MN 4; Friedmann (n 31) 287.

34 Wright (n 24) 12.

35 Albrecht Randelzhofer and Oliver Dörr, 'Article 2(4)' in Bruno Simma et al (ed), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012), MN 37 and 39.

of states'.[36] Remarkably, that author notes that espionage would, though, not be an 'international crime',[37] a term of art in international law referring to serious atrocities like genocide, war crimes, crimes against humanity and the crime of aggression. In the matter the contrary can be argued, namely that espionage is a 'tool that enables functional cooperation'[38] between States. In other words, espionage can help to better understand the other States' security needs and concerns, to build up trust, and consequently to facilitate international dialogue.[39] It can be also argued that espionage supports a 'super-validation' of compliance with international obligations relevant to international peace and security by other States, offers confirmation of the legitimacy of assurances provided, and thus can support the willingness of States to cooperate.[40]

Some commentators, incorrectly expanding the definition of espionage to include 'covert military assistance', attest that espionage would violate the principle of non-intervention[41] in the domestic affairs of other States. In this sense, the US support to the *contras* in Nicaragua in the 1980s is referred to as an 'undoubted example[s] of espionage [...] that exceed the non-interference standard.'[42] In this context another US-specific term, also used by legal commentators and interfusing espionage with other activities, needs to be mentioned, namely 'preparation of the battlefield' that is conducted by military forces in close cooperation with the intelligence community. The notion of 'covert military assistance' (also called 'covert action' or 'covert operation') and 'preparation of the battlefield' both display a US-specific operational terminology which is blurring the line between espionage and other covert activities, which need to be distinguished even if conducted during the same (military) operation. A forbidden intervention in domestic affairs requires the element of coercion of the other State.[43] Scholars assert that illegal coercion implies massive influence, inducing the affected State to adopt a decision with regard to its policy or practice which it would not entertain as a free and sovereign State.[44] It is clear that clandestine information gathering as such will not fulfil such requirements.

Partly, it is claimed that because a State's economy is part of its internal affairs, and economically motivated espionage is an activity by which one State intervenes in

36 Delupis (n 24) 67.

37 cf ibid 68.

38 Baker (n 25) 1112.

39 ibid 1105.

40 ibid 1092, 1104ff and 1108.

41 See Terry D Gill, 'Non-Intervention in the Cyber Context' in this volume.

42 Forcese (n 26) 198.

43 See discussion at Philip Kunig, 'Intervention, Prohibition of' in Rüdiger Wolfrum (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press 2008, online edition [www.mpepil.com]) [in following MPEPIL] MN 5ff.

44 Kunig (n 43) 22-27; Ulrich Beyerlin, 'Intervention' in Rüdiger Wolfrum and Christiane Philipp (ed), *United Nations: Law, Policies and Practice* (vol I, CH Beck 1995) para 8-9.

another State's economic affairs, such espionage is illegal.[45] In general terms, it can be asserted that the internal affairs of a State (*domaine réservé*) describe areas not regulated by international norms or not being of some common interest or value.[46] In times of globalisation and worldwide economic interdependence, it can be argued that only the realm of strategic and political decisions with regard to a State's economy is part of the *domain réservé*. Here, again, espionage, even if targeting respective strategic or political information of economic nature, would not *per se* show the aspect of 'coercion' and thus not violate the non-intervention principle.

Notably, international law provisions regulating privacy and secrecy of correspondence do not establish any restrictions on State espionage targeting data saved or temporarily available on servers located on foreign territories, and therefore do not establish the illegality of inter-State or 'extraterritorial' espionage. Article 17(1) of the *International Covenant on Civil and Political Rights* of 1966, obliging States to protect individuals against 'interference with [...] privacy [...] or correspondence' applies, pursuant to Article 2(1) to 'individuals within [the State's ...] territory and subject to its jurisdiction' only. The same applies to the respective provisions of Article 8(1) of the *European Convention on Human Rights* of 1950 (Article 1: 'within their jurisdiction'), Article 11(2) of the *American Convention of Human Rights* of 1969 (Article 1(1): 'all persons subject to their jurisdiction') and Article 21(1) of the *Arab Charter of Human Rights* of 2004 (Article 2: 'within its territory and subject to its jurisdiction'). Also Article 18(b) of the *Cairo Declaration on Human Rights in Islam* of 1990 refers to privacy and secrecy of correspondence; however, it has the nature of a 'general guidance for Member States' (para. 6 of the Preamble). (Interestingly, the *African [Banjul] Charter on Human and Peoples' Rights* of 1981 does not contain respective rights.) The *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* of 1980, elaborated under the auspices of the Organisation for Economic Co-operation and Development, which might be considered 'soft law',[47] are also applicable only within the State's own sovereign area. According to Article 37(1) of the *Constitution of the International Telecommunication Union* of 1992 Member States shall take all possible measures 'ensuring the secrecy of international correspondence', however, only within own territory or area under jurisdiction. Overall it can be determined that 'extraterritorial' spying on citizens, companies or governments is not forbidden as such by international and regional human rights law.[48] Even if the treaties could be interpreted[49] as establishing an obligation on Member States to protect individuals

45 Sepura (n 2) 145.

46 Kunig (n 43) 3; Beyerlin (n 44) 7; cf Georg Nolte,'Article 2(7)' in Simma (n 35) 27; Katja S Ziegler, 'Domaine Réservé' in MPEPIL (n 43) MN 1.

47 cf Forcese (n 26) 195.

48 ibid 208; Wiliams (n 26) 1177.

49 See Dinah PoKempner, 'Cyberspace and State Obligations in the Area of Human Rights' in this volume, section 6.

within their territory and jurisdiction from foreign countries' espionage endeavours,[50] such an obligation would apply towards own citizens, and would still not establish a prohibition of information gathering by foreign States. With regard to data transiting through internet routers and IXPs or saved in 'clouds' located in the spying State's sovereign area, the international and regional human rights treaties do not establish a general prohibition of espionage activities, as the rights to privacy and secrecy of correspondence are not absolute and can be interfered in accordance with national law as necessary for national security, public safety, etc.[51] Thus, there will be specific limitations on espionage activities conducted by a State on its own territory or area under exclusive jurisdiction, which, however, derive from the respective national laws and not from public international law.

Finally, to address the specific case of industrial espionage, the international rules governing property rights protection do not contain a prohibition of espionage.

The *Paris Convention for the Protection of Industrial Property* of 1883 (subsequently amended)[52] governs international patents and trademarks. Article 10*bis*(1) of the Convention obliges Member States to assure national protection against 'unfair competition'. The provision defines 'unfair competition', but the Convention does not mention that acquiring proprietary information qualifies as such.[53] In the opinion of scholars and Member States, the provision does not prohibit economic espionage.[54]

The *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS) of 1994 imposes in Article 39(1) an obligation on Member States to 'protect undisclosed

---

50 Interestingly, a recent UN GA draft resolution introduced by Brazil and Germany proposes to: *'[r]equest[s]* the United Nations High Commissioner for Human Rights to submit an interim report on the protection of the right to privacy in the context of domestic *and extraterritorial* surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection of personal data, [...], and a final report [...], with views and recommendations, to be considered by Member States, with the purpose of identifying and clarifying principles, standards and best practices on how to address security concerns in a manner consistent with States' obligations under international human rights law and with full respect for human rights, in particular with respect to surveillance of digital communications and the use of other intelligence technologies that may violate the human right to privacy and freedom of expression and of opinion', Brazil and Germany, draft resolution 'The right to privacy in the digital age', UN Doc A/C.3/68/L.45 (1 November 2013) [emphasis added].

51 see Article 17(1) of the *International Covenant on Civil and Political Rights* refers only to 'arbitrary or unlawful interference'; Article 8(2) of the *European Convention on Human Rights* prohibits 'interference [...] except such as is in accordance with the law and is necessary [...] in the interests of national security, public safety [...] [et al.]'; Article 11(2) of the *American Charter on Human Rights* prohibits interference that would be 'arbitrary or abusive'; Article 18(b) of the *Cairo Declaration* prohibits 'arbitrary interference'; Article 21(1) of the *Arab Charter Human Rights* 'arbitrary or unlawful interference'; Article 37(2) of the *Constitution of the International Telecommunication Union* states that 'secrecy of international correspondence' is subject to 'the application of [the Member States'] national laws'.

52 As revised at Brussels on 14 December 1900, at Washington on 2 June 1911, at The Hague on 6 November 1925, at London on 2 June 1934, at Lisbon on 31 October 1958, and at Stockholm on 14 July 1967, and as amended on 28 September 1979; administered by World Intellectual Property Organization (WIPO).

53 Christopher G Blood, 'Holding Foreign Nations Civilly Accountable for Their Economic Espionage Practices' (2002) 42 IDEA – The Journal of Law and Technology 228, 234.

54 Sepura (n 2) 143.

information' and 'data submitted to governments or governmental agencies'. Paragraph 2 grants 'natural and legal persons' the right to 'prevent[…] information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices'. 'Honest commercial practices' are further specified in footnote 10 as including 'breach of confidence', but the definition does not include the unlawful taking (or copying) of proprietary information.[55] Thus, certain types of information relating to intellectual property rights, including trade secrets, might be protected by TRIPS, but only in the form of an obligation on Member States to protect such information within their respective territory.[56] TRIPS does not protect trade secrets against espionage by a foreign State; it does not outlaw economic espionage on the international level.[57]

The World Intellectual Property Organization (WIPO) *Copyright Treaty* of 1996 (WCT) (according to Article 1 being a special agreement within the meaning of Article 20 of the *Berne Convention for the Protection of Literary and Artistic Works* of 1886, subsequently amended[58]) protects computer programs (Article 4) and databases (Article 5). WCT obliges Member States to provide effective legal protection of copyright holders' rights, including against the circumvention of technological measures (e.g., encryption) used by the authors in connection with the exercise of their rights and against the removal or altering of information, such as certain data that identify works or their authors.[59] The obligation to provide legal remedies for copyright protection applies with respect to each Member State and its sovereign area, and does not establish a prohibition against espionage by foreign States.

Member States of the World Trade Organization (WTO), i.e. the organisation dealing with global rules of trade between States, have shown no interest in addressing economic espionage despite mounting worries about its practice.[60] States party to these treaties knowingly tolerate foreign States' economic espionage, which might be based upon the notion of preserving such a possibility for themselves.

55 Also ibid 144, Blood (n 53) 235.

56 David P Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies' (ASIL insights, 20 March 2013, vol 17, issue 10) <http://www.asil.org/pdfs/insights/insight130320.pdf>.

57 Also Blood (n 53) 235, Gerald O'Hara, 'Cyber-Espionage: A Growing Threat to the American Economy' (2010-2011) 19 CommLaw Conspectus 242, 244 and 256.

58 Revised at Paris in 1896 and at Berlin in 1908, completed at Berne in 1914, revised at Rome in 1928, at Brussels in 1948, at Stockholm in 1967 and at Paris in 1971, and as amended in 1979.

59 See WIPO, Summary of the WIPO Copyright Treaty (WCT) <http://www.wipo.int/treaties/en/ip/wct/summary_wct.html.>.

60 Fidler (n 56).

2.2 Legality of Espionage

Those who deem espionage expressly permitted under international law partly claim it to be a component of the right of anticipatory or pre-emptive self-defence, and therefore a necessary means whereby States defend themselves.[61] As a supporting argument, it is referred to the fact that in the context of the 'Gary Powers U-2 incident'[62] in 1960, the US Secretary of State justified the act of espionage on Soviet territory as a measure to 'lessen and to overcome danger of surprise attack'.[63] If this line of argument is followed, any act of espionage would derive its legality from the spying State's motivation (i.e., the right to anticipatory self-defence, as opposed to preparations for an act of aggression) which is a legal construct not acceptable.[64] Importantly, and introducing a notion of logic, the legality of espionage cannot be derived from the right to self-defence, as espionage activities would be conducted chronologically before the right to self-defence was triggered by an actual or imminent armed attack in the meaning of Article 51 of the UN Charter.[65]

Also, any reference to specific provisions[66] of arms control treaties, establishing the right of the parties to collect intelligence with respect to assurance of the compliance with the arms control obligations in question; to confidence building measures[67]

---

61 Alexander Melnitzky, 'Defening America against Chinese Cyber Espionage Though the Use of Active Defences' (2012) 20 Cardozo Journal of International and Comparative Law 538, 564; Sulmasy and Yoo (n 25) 636; Baker (n 25) 1095f (with further references); James E Baker, 'What's International Law Got To Do With IT? Transnational Law and the Intelligence Mission' (2007) 28 Michigan Journal of International Law 656; Scott (n 26) 224.

62 'U-2' was a US photo-reconnaissance airplane. Between 1956 and 1960, U-2 flights regularly crossed Soviet territory. In 1960 a U-2 was shot down over the Soviet territory and the pilot, the CIA contractor Gary Francis Powers, was captured. The U-2 aircraft lacked identification; the pilot Powers was not wearing a uniform, but was in possession of an identity card marked 'Defence Department, US'. The US admitted the espionage activity and defended the conduct on the basis of past Soviet practice of employing secret agents, additionally asserting that the US would have a duty towards the 'free world' to spy on the Soviet Union. The Soviet Union addressed the over-flight as such and justified the shooting of the aircraft on the grounds of self-defence, claiming that a single plane was capable of carrying weapons of great destructiveness. cf Edmondson (n 26) 447 (with further references); Demarest (n 26) 340f; Barrie (n 26) 248.

63 Cited by Wright (n 24) 17f; Baker (n 25) 1095 in fn 20.

64 cf Baker (n 25) 1097.

65 cf Forcese (n 26) 199.

66 cf Williams (n 26) 1177; Simon Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 Michigan Journal of International Law 1072, 1090ff; eg Article XII(1) of the *Treaty on the Limitation of Anti-Ballistic Missile Systems* of 1972, Article V of the *Strategic Arms Limitation Treaty* (SALT I) of 1972 as well as Article XII(1) of the *Treaty on the Elimination of Intermediate-Range and Shorter Range Missiles* of 1987 (all concluded between USA and USSR) stated: 'For the purposes of providing assurance of compliance with the provisions of this Treaty [...] each Party shall use national technical means of verification at its disposal consistent with generally recognized principles of international law.' Article III-VI of the *Strategic Arms Limitation Treaty* (SALT II) of 1991 allows the collection of imaginary. Articles I(1) and II(4) of the *Treaty on Open Skies* of 1992 foresee aerial observation flights. Article III(1) of the *London Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof* of 1971 foresees verification measures through observation.

67 Kish (n 25) 86ff.

providing, for example, for the exchange of military observers; to the lawful presence[68] of armed forces of a Member State of an Alliance on the territory of another Ally, such as in the context of the NATO *Status of Forces Agreement*; or to information sharing arrangements[69] cannot be understood as an indication of a general legality of espionage activities. Admittedly, respective agreements and arrangements do expressly or implicitly provide for possibilities of intelligence gathering or of 'strategic observation' on another State's territory. However, such activities cannot be considered as inter-State espionage. Apart from the case of information sharing arrangements, which must be deemed cognisant cooperation activities, the examples given by the respective legal commentators describe information gathering which might be conducted under secrecy in particular cases, but nevertheless is generally consented to by the other State(s).

Furthermore, advocates of the lawfulness of espionage refer to the widespread State practice, particularly the existence of government intelligence agencies proving espionage services as a legitimate function of a State, and to the lack of official statements of illegality of espionage, thus indirectly insinuating legality under international customary law.[70] Despite some criticism[71] of the logic of the phrasing, it is generally accepted in scholarly writings[72] and confirmed by the ICJ[73] that the identification of a rule of 'international custom, as evidence of a general practice accepted as law', as stated in Article 38(1)(b) of the ICJ Statute requires two elements: (1) a generally uniform and consistent State practice and (2) the *opinio iuris sive necessitatis*, i.e., the belief that the behaviour is required or permitted under international law. Certainly, there is extensive State practice of espionage, because espionage is widely accepted as a common, inherent and established function of a State.[74] However, that practice is not accompanied by government statements which could allow any inference as to the assessment of the legality or illegality of such activities (*opinio iuris*), for which the following (non-exhausting) examples can be presented.

With regard to traditional politically motivated espionage, the 'Gary Powers U-2 incident' of 1960[75] resulted in official protests from the Soviet Union referring to the intrusion into its airspace by the US intelligence aircraft.[76] The 'USS Pueblo incident'

68 ibid 87ff.

69 Williams (n 26) 1177; Chesterman (n 66) 1090ff.

70 eg Smith (n 25) 544; Baker (n 25) 1094.

71 cf Pellet (n 31) 207; Wolfrum (n 72) 24.

72 eg Rüdiger Wolfrum, 'Sources of International Law' in MPEPIL (n 43) 25; Tullio Treves, 'Customary International Law' in MPEPIL (n 43) 17ff (with references to ICJ jurisprudence); Pellet (n 31) 201; cf Crawford (n 30) 23-30 (detailed discussion of the elements of customary international law).

73 eg *North Sea Continental Shelf,* Judgement (1969) ICJ Rep 3, para 77.

74 Kish (n 25) XV; Demarest (n 26) 321.

75 See n 62.

76 See Union of Soviet Socialist Republics, Draft Resolution [Concerning Alleged Aggressive Acts by the United States Air Force Against the Soviet Union] UNSC Doc S/4321 (23 May 1960) (not adopted). The draft resolution condemns the intrusion into Soviet territory as an act of aggression.

of 1968, resulting in a written admission of espionage activities by the US against North Korea, did not trigger any official statement about the legality or illegality of the actions.[77] During the mediations by the UN Secretary General between France and New Zealand in the context of the 'Rainbow Warrior incident' of 1985,[78] the issues discussed, as far as is known, addressed questions of attack and violation of territorial sovereignty.[79] Also the grounding of a Soviet submarine in a Swedish military protection area in 1981 resulted in issuing of diplomatic protest notes by the Swedish government, which did not refer to espionage as such, but rather to environmental concerns and territorial aspects.[80]

With regard to economic espionage, reportedly, the discovery of French spies trying to collect trade secrets from foreign subsidiaries of the US computer companies IBM and Texas Instrument between 1987 and 1989 resulted in a letter of diplomatic protest from the US to France.[81] The discovery that Israeli intelligence officers stole technological information on an airborne spy-camera system from the US Department of Defense (DoD) contractor Recon Optical in 1992 did result in a denial by Israel and was not, as far as is publicly known, followed by any official statement by the US government.[82] In general, despite recurring reports from US Central Intelligence Agency (CIA) identifying over 90 countries who have conducted economic espionage against US companies, the US government has been reluctant to publicly 'name and shame' foreign governments.[83]

77 'USS Pueblo' was an intelligence ship armed with two machine guns. It was classified as a warship and as a commissioned vessel in the US naval register. The crew wore US Navy uniforms. On 23 January 1968 the vessel was seized by North Korean warships in international waters off the coast of North Korea. US signed a document admitting espionage in order to have the crew released, which was retracted in the aftermath. The ship is still held captive today. See Barrie (n 26) 249.

78 On 10 July 1985 French agents sunk a civilian vessel used by Greenpeace at its mooring in the harbour of Auckland, New Zealand, which resulted also in the death of a Dutch national. The agents were acting upon orders of the French Directorate General of External Security. They had entered the New Zealand territory covertly. For the subsequent arbitration (following the mediation by UN Secretary General) see *Rainbow Warrior* Arbitral Award (1990) XX RIAA 215-284.

79 Barrie (n 26) 250ff.

80 On 27 October 1981 a Soviet submarine grounded on a shoal in Swedish internal waters, inside the military protection area of the Karlskrona naval base. The Swedish government issued diplomatic protest notes addressing 'illicit activities' and carrying nuclear weapons. See Delupis (n 24) 53.

81 Sepura (n 2) 142; Michael Wines, 'French Said to Spy on U.S. Computer Companies' *The New York Times* (18 November 1990) <http://www.nytimes.com/1990/11/18/world/french-said-to-spy-on-us-computer-companies.html >.

82 Sepura (n 2) 142. A respective article by Edward T Pound and David Ro in the *Wall Street Journal* of 22 January 1992 is no longer available.

83 Brenner and Crescenzi (n 2) 399. For an overview of economic espionage events 1945-2006 see: ibid 401-413; US Office of the National Counterintelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace' (Report to the Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011).

With regard to cyber espionage, neither the 'Moonlight Maze'[84] incident of 1998-1999, nor the 'Titan Rain'[85] incident of 2003-2007 resulted in any official statements by the US towards the States suspected of sponsoring the activities (Russia and China) nor by those suspected States, which would provide an indication of an *opinio iuris* with regard to the legality or illegality of cyber espionage. In 1998, the publication of an European Parliament (EP) research paper on the US and United Kingdom (UK) espionage program based on the ECHELON interception system, 'indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex to find key words' and 'designed for primarily non-military targets: governments [...] in virtually every country',[86] did not result in any notable reactions by EU Member States; neither did an official EP report issued in 2001.[87] A more recent and widely noticed case was the 2003 leakage of the concerted effort of the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) to tap into the office and home communications (phone and email) of the delegations of the other thirteen members of the UN Security Council, as well as monitoring the communications of the UN Secretary General in order to collect information on positions in the debate about the military action against Iraq.[88] The only publicly perceivable consequence was that the UN, referring to diplomatic immunity regulations only, reportedly stated its wish to 'contact' the US over the reports.[89] In 2013 the 'discovery' of the PRISM and the globally operating 'Boundless Informant'

84 Hackers, supposedly from Russia, penetrated computer networks of the US DoD, NASA, Department of Energy, military contractors and military-civilian universities, cf Christopher C Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 European Journal of International Law 825, 840ff (with further references); Schaap (n 26) 141.

85 Supposedly Chinese State-sponsored hackers gained access to many United State Departments and to defence contractor computer networks which were targeted for their sensitive information, such as information on aviation and flight-planning software from the Redstone Arsenal of the US Army Aviation and Missile Command. See eg Bradley Graham, 'Hackers Attack Via Chinese Web Sites' *The Washington Post* (25 August 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html >.

86 European Parliament, 'An Appraisal of Technologies of Political Control' (Directorate General for Research, Scientific and Technological Options Assessment, Working Document, PE 166 499, 6 January 1998) 19 <http://cryptome.org/stoa-atpc.htm> ('The ECHELON system forms part of the UKUSA system but unlike many of the electronic spy systems developed during the cold war, ECHELON is designed for primarily non-military targets: governments, organisations and businesses in virtually every country. The ECHELON system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex to find key words. Five nations share the results with the US as the senior partner under the UKUSA agreement of 1948, Britain, Canada, New Zealand and Australia are very much acting as subordinate information services.').

87 European Parliament, *Report on the existence of a global system for the interception of private and commercial communications* (ECHELON interception system, 2001/2098(INI), Doc No A5-0264/2001 PAR1, 11 July 2001) <http://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_en.pdf>.

88 eg Martin Bright, Ed Vulliamy and Peter Beaumont, 'Revealed: US dirty tricks to win vote on Iraq War' *The Guardian / The Observer* (2 March 2003) <http://www.theguardian.com/world/2003/mar/02/usa.iraq>; Patrick E. Tyler, 'Ex-Aide to Blair Says the British Spied on Annan' *The New York Times* (27 February 2004) <http://www.nytimes.com/2004/02/27/world/ex-aide-to-blair-says-the-british-spied-on-annan.html>.

89 Reuters, 'United Nations says it will contact U.S. over spying report' *Chicago Tribune News* (2 August 2013) <http://articles.chicagotribune.com/2013-08-26/news/sns-rt-us-usa-security-nsa-un-20130825_1_michelle-nichols-u-n-spokesman-farhan-haq-u-s-intelligence>.

programmes,[90] clandestine electronic surveillance programs operated by the US NSA since 2007, providing mass-surveillance of citizens and government members in- and outside the US, lead to some political tensions,[91] but they focussed on citizens' rights to privacy and data protection and, with regard to alleged surveillance of Heads of Government's mobile phones, to political trust relationships.[92] Allegations of the general legality or illegality of espionage under international law were at no time perceivable. As to other major cases of cyber espionage such as *Operation Red October*,[93] an attribution to a State is illusory, and any official statement from a target State in terms of *opinio iuris* is not to be expected.

Overall, the *usus* on the inter-State level with regard to espionage, by either traditional or cyber means, seems to be a 'policy of silence'. If any official statements are perceivable to the public at all, protest, mostly in cases of spying by diplomatic staff,[94] and denial seem to be the 'most accepted ritual'.[95] However, the number of formal protests was hitherto irrelevant.[96] Official statements by States referring either to the legality or illegality of peacetime espionage conducted by States are not to be found. Interestingly, one scholar thus stated that 'state practice and *opinio juris* appear to run in opposite directions', especially referring to a 'disconnection' between widespread practice of espionage by States and penalisation under domestic law.[97] However, differentiating between the international and national law levels, which are interconnected by 'principles of law recognized by civilized nations', an *opinio iuris* cannot be derived from State practice alone which, in theory, can be either in violation of or confirming a certain rule of international custom, and can also not be seen as insinuated by the practice of national

90 See *supra* note 12.

91 cf *Spiegel* online international, 'Growing Alarm: German Prosecutors to Review Allegations of US Spying' (30 June 2013) <http://www.spiegel.de/international/germany/german-prosecutors-to-review-nsa-spying-allegations-a-908636.html>; Dave Neal, 'European Parliament votes for PRISM snooping investigation' *The Inquirer* (9 July 2013) <http://www.theinquirer.net/inquirer/news/2280187/european-parliament-votes-for-prism-snooping-investigation>.

92 eg Alison Smale, 'Anger Growing Among Allies on U.S. Spying' *The New York Times* (23 October 2013), <http://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html?_r=0>; European Parliament, 'Prism: MEPs hit out at US surveillance of people's personal data' *European Parliament News* (11 June 2013) <http://www.europarl.europa.eu/news/en/headlines/content/20130611STO11522/html/Prism-MEPs-hit-out-at-US-surveillance-of-people's-personal-data>.

93 See *supra* note 11. A highly sophisticated and resistant worm which since 2007 has targeted the computer network equipment and mobile devices (Windows Mobile, iPhone, Nokia) of governments, embassies, nuclear and energy research entities, oil and gas companies and many more, or the even more sophisticated, recently discovered cyber espionage software harvesting years of communication data of the Finish Ministry of Foreign Affairs with other countries. Keir Giles, 'Opinion: Cyber attack on Finland is warning for EU' *eureporter* (12 November 2013) <http://www.eureporter.co/frontpage/2013/11/12/opinion-cyber-attack-on-finland-is-warning-for-eu/>.

94 DoD Office of Legal Counsel, 46 ('[...] there has been almost no activity concerning peacetime espionage within the international legal system except for public complaints and the expulsion of implicated diplomats').

95 Edmondson (n 26) 445.

96 McDougal, Lasswell and Reisman (n 25) 394.

97 Chesterman (n 66) 1072.

criminal law enactment and enforcement activities. In contrast to the assertions of some legal commentators, the consistent State practice of espionage activities and the lack of *opinio iuris* on its illegality do not constitute the practice's (positive) legality.

Finally, it is sometimes claimed within scholarly writings that espionage conducted in certain 'common spaces' would derive (positive) legality from the legal regimes governing those areas. The respective lines of argument are worth presenting, as they could prove to be relevant to cyberspace, as another 'common space', and thus to cyber espionage.

Article VII(3) of *The Antarctic Treaty* of 1959 foresees 'inspections' of stations, installations, equipment, ship and aircraft by national observers in the Antarctica. According to Article VII(1) the inspections serve the purpose of verification of compliance with the provisions of the treaty, such as the prohibition of military activities (Article I(1)) or radioactive pollution (Article V(1)). It was asserted that the 'scope of reconnaissance [regulated by *The Antarctic Treaty*] manifests the permissibility of espionage in Antarctica.'[98] Similarly, Article XII of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* of 1967 foresees 'visits' by all Member States to all stations, installations, equipment and space vehicles on the moon and other celestial bodies (on a basis of reciprocity). Additionally, Article 15(1) of the *Agreement Governing the Activities of States on The Moon and Other Celestial Bodies* of 1979 establishes the right to inspections by all Member States of all space vehicles, equipment, facilities, stations and installations on the moon for purposes of verification of the compliance of other States with the treaty. Also in this regard, it was asserted within scholarly writings that 'the regime of reconnaissance [...] manifests the permissibility of espionage in outer space and on celestial bodies.'[99] Of course these inspections provide for information gathering which is not generally done in secrecy or under disguise, and therefore the legality of espionage in Antarctica or in, or from, outer space cannot be derived from these regulations.

As a supporting argument with regard to outer space, it has been asserted that these international treaties would not prohibit surveillance satellites and no State has formally protested against their use.[100] Indeed, even the UN uses satellite technology for purposes of information gathering,[101] although the (non-binding) UN GA Resolution

98 Kish (n 25) 114.

99 ibid 120.

100 Chesterman (n 66) 1085.

101 see United Nations Institute for Training and Research (UNITAR) Operational Satellite Applications Programme (UNOSAT) implemented in co-operation with the European Organization for Nuclear Research (CERN). The programme, created in 2000, provides satellite solutions to humanitarian aid and sustainable development organisations and comprises UN fieldworkers, satellite imagery experts, geographers, geologists, sustainable development experts, database programmers and internet communication specialists. Their stated mission is 'to deliver integrated satellite-based solutions for human security, peace and socio-economic

Principles Relating to Remote Sensing of the Earth from Outer Space[102] of 1986 could be interpreted[103] as having been intended to exclude surveillance for espionage purposes. However, the practice by States and international organisations of using intelligence satellites does not provide any further clarification as to the legality of information gathering from outer space in terms of international customary law, as it is not accompanied by respective *opinio iuris*.

Furthermore, the legality of espionage on the high seas, the air above and the deep seabed and its subsoil was asserted as deriving from the freedom of the high seas (see Article 87 of the *United Nations Convention on the Law of the Sea* of 1982 – UNCLOS).[104] This opinion is equally asserted to be confirmed by extensive State practice. [105] However, the freedom of the high seas does neither expressly permit nor prohibit espionage activities; and due to the lack of publicly perceivable *opinio iuris* on the legality of espionage activities as deriving from the freedom of the high seas, a conclusion cannot be made.

Overall, although international law does not prohibit peacetime espionage as such (see section 2.1), the (positive) legality of peacetime espionage cannot be determined.

2.3 Specific Restraints on Espionage

Notwithstanding the above findings with regard to the general legality or illegality of peacetime espionage, international law contains a few regulations merely restraining espionage activities in rather specific situations.

Such limitations are endorsed in the *Vienna Convention on Diplomatic Relations* of 1961 (VCDR), the *Vienna Convention on Consular Relations* of 1963 (VCCR) and the *Convention on Special Missions* of 1969 (CSM), widely seen as partly codifying and partly developing international customary law.[106] Diplomatic and consular law provides for the inviolability of official 'archives and documents [...] at all times and wherever they may be', as well as of 'official correspondence of the mission' (Articles 24 and 27(2) of the VCDR, Articles 33, 35(2), 58 and 61 of the VCCR and Articles 26 and 28(2) of the CSM). Those regulations provide protection against espionage activities, including cyber espionage, by the receiving State. They apply to official email communication as a form of 'correspondence', to documents saved in electronic form

development, in keeping with the mandate given to UNITAR by the UN General Assembly since 1963', see <http://www.unitar.org/unosat/who-we-are> and <http://www.unosat.org/>.

102 UN GA Res 41/65 (3 December 1986), Annex.

103 Chesterman (n 66) 1086.

104 Kish (n 25) 104f and 109.

105 ibid 105f (naming, e.g., the surveillance of the Portuguese ship 'Santa Maria' (seized by revolutionaries) in 1961 by US and UK armed forces until its entrance into territorial waters of Brazil – however, upon Portuguese request; the surveillance by UK armed forces of the Libyan tanker 'Torrey Canyon' which run aground on the Seven Stones reef).

106 Horst Fischer, 'Diplomatische und konsularische Beziehungen' in Ipsen (n 29) § 35 MN 3ff, § 38 MN 2.

and, in a broad interpretation, to databases of a mission, being a new form of 'archives', saved on any server (e.g., in a 'cloud') located on the territory of the receiving State. Seen in conjunction with the general and broadly stated obligation of the receiving State to protect the premises of a mission against 'any intrusion' and to prevent 'any disturbance of the peace of the mission or impairment of its dignity' (Article 22(2) of the VCDR, Articles 31(3) and 59 of the VCCR, and Article 25(2) of the CSM), a wide interpretation of these provisions seems justified. Notably, diplomatic law does not provide a prohibition against espionage activities against diplomatic and consular missions, documents, databases and communication by a third State (i.e., other than the receiving State). The extensive practice of espionage against diplomatic and consular installations by receiving States does not, in contrast with some allegations by US commentators,[107] change the law.

It is not unusual that diplomatic or consular staff conduct espionage activities on the territory of the receiving State.[108] However, such activities violate the spying personnel's duty 'to respect the laws and regulations of the receiving state' and to refrain from using the premises of the missions 'in any manner incompatible with the functions[109] of the mission' (Article 41(1) and (3) of the VCDR, Article 55(1) and (2) of the VCCR and Article 47(1) and (2) of the CSM). The consequence foreseen by the 'self-contained'[110] regime of diplomatic law is for the receiving State to declare the spying staff member a *persona non grata* (*quasi* expulsion followed by withdrawal of the personnel by the sending State, see Article 9 of the VCDR, Article 23 of the VCCR and Article 12 of the CSM).[111] Remarkably, such declarations are not accompanied by official statements expressing the *opinio iuris* that espionage as such would be illegal under international law, but refer usually, if at all, to activities 'incompatible with the functions of the mission'. Interestingly, most of the declarations of diplomats as *personae non gratae* were issued, at least until the end of the Cold War, for espionage activities on the receiving State's territory.[112]

107 Smith (n 25) 545 (Smith is former General Counsel of the CIA).

108 McDougal, Lasswell and Reisman (n 25) 380ff; Chesterman (n 66) 1087 ('Diplomacy and intelligence gathering have always gone hand in hand.')

109 Legitimate functions of a mission are set out in Article 3 of the VCDR and Article 5 of the VCCR; according to Article 3 of the CSM, the functions of a special mission are determined by mutual consent of the sending and receiving State.

110 *United States Diplomatic and Consular Staff in Tehran,* Judgment (1980) ICJ Rep 3, para 86.

111 Chesterman (n 66) 1088ff.

112 Holger P Hestermeyer, 'Vienna Convention on Diplomatic Relations (1961)' in MPEPIL (n 43) MN 20. Since the 1990s the declarations of *persona non grata* for spying by diplomats declined (examples are withdrawal of four British diplomats from Russia in 1996 and expulsion of 50 Russian diplomats by the US in 2001). Although such cases continue to occur, the declarations are increasingly triggered by (alleged) involvement of diplomatic staff in terrorist and subversive activities (e.g., expulsion of Iranian diplomats by Argentina linked to the bombing of the Argentine Jewish Mutual Aid Association in 1994).

Furthermore, the international law of the sea restrains espionage activities in certain situations. According to Article 19(1) of the UNCLOS, ships may not engage in activities that would be 'prejudicial to the peace, good order or security of the coastal State' during an innocent passage through the territorial sea of another State. According to paragraph 2 of the provision such activities would, *inter alia*, consist of:

- 'any act aimed at collecting information to the prejudice of the defence or security of the coastal State' (lit. c);
- 'the carrying out of research or survey activities' (lit. j); and
- 'any act aimed at *interfering with any systems of communication* [...] of the coastal State' (lit. k) [emphasis added].

Those activities would certainly preclude the conduct of cyber espionage. Pursuant to Article 45 of the UNCLOS, the above-mentioned prohibitions also apply to the exercise of the right of transit passage through international straits. Similar prohibitions, namely 'refrain[ing] from any activities other than those incident to […] [the] normal modes of continuous and expeditious transit' (Article 39(1)(c) of the UNCLOS), apply to ships and aircraft in transit passage or in archipelagic sea lanes passage (Article 54 of the UNCLOS). Additionally, during such passage ships 'may not carry out any research or survey activities without […] prior authorization […]' (Article 40 of the UNCLOS).

Another international agreement limiting espionage activities is the NATO *Status of Forces Agreement* (SOFA). In Article II, the agreement states 'the duty of a force and its civilian component and the members thereof as well as their dependents to respect the law of the receiving State'. Although the duty to 'respect' the laws of the States receiving the armed forces of an Ally is to be distinguished from 'observing' or 'obeying' domestic laws, it can be asserted that the obligation deriving from Article II will be violated in cases of espionage activities (which are penalised in all national laws of NATO Member States).

It needs to be emphasised that the punctual prohibitions of espionage as presented, applying in certain circumstances only, do not allow any conclusion about the general legality or illegality of peacetime espionage, as they could present either an exception from or an explicit confirmation of a general rule.

2.4 Intermediate Result: Not Forbidden or *non liquet*

Overall, the author of this chapter concurs with those legal commentators who state that public international law is silent about State espionage during peacetime. An analysis of international jurisprudence does not allow a conclusion to the contrary. The ICJ has not taken a position on the (il)legality of espionage, although it has had the opportunity to do so on a few occasions.[113] In the *Nicaragua* case, Nicaragua has complained of

[113] cf Fleck (n 26) 691.

overflights of its territory by US aircraft, among others, for purposes of intelligence gathering.[114] However, Nicaragua only referred to the infringement of its airspace.[115] The Court did consider the overflights as violations of Nicaragua's airspace and thus its territorial sovereignty.[116] At no time did the Court refer to the legality or illegality of espionage as such. In the *Hostages* case the Iranian Foreign Minister referred to alleged espionage by US diplomats. The Court did not accept those allegations as a justification for Iran's conduct (i.e., allowing a group of militants to attack and occupy the US Embassy by force, to seize the diplomatic and consular staff as hostages, and endorsing that action) and merely referred to the remedies the 'self-contained' regime of diplomatic law offers in such cases.[117] Again, the Court did not address the question of the legality or illegality of peacetime espionage.

The classic international law approach to a situation which is not (or only partly) regulated by law would be to invoke the basic principle stated in 1927 by the Permanent Court of International Justice (PCIJ) in the *Lotus*[118] case: based on the notion of State sovereignty, in the absence of a legal prohibition, a State enjoys a rebuttable presumption of freedom of action. On the contrary, the consensual approach to international law assumes that in case of lack of a regulation a legal *lacuna* is present from which such permission cannot be derived.[119] The situation in question would need to be deemed simply unregulated by international law (*non liquet*).[120] Thus, espionage is either permitted, because it is not forbidden (based on the notion of State sovereignty) or it is not regulated and therefore not justiciable (i.e., accessible to a decision on its legality or illegality) under international law (*non liquet* based on consensual approach to international law).

In conclusion, States are free to conduct ('extraterritorial') peacetime cyber espionage activities. While the means used to gain access to the targeted data may violate international law, the copying of data itself does not.

3. New Tendencies in International Law

Espionage activities are by no means new phenomena; they have always targeted valuable information of a political and economic nature, and their conduct and, with regard to espionage by other States, prevention has always been in national interest. However, the emergence of cyber espionage seems to have changed the picture. The respective shift in the perception of (economically motivated) espionage as relevant to national

114 *Military and Paramilitary Activities in and against Nicaragua,* Merits (1986) ICJ Rep 14, para 21.

115 ibid, paras 87 and 250.

116 ibid, paras 91, 251 and 252.

117 Hostages case (n 110) para 85-87.

118 *The Case of the S.S. 'Lotus'* (Merits) [1927] PCIJ Rep Ser A, No 7, 18.

119 Wolff Heintschel von Heinegg, 'Die weiteren Quellen des Völkerrechts' in Ipsen (n 29) § 19 MN 8.

120 ibid.

security (3.1) might explain recent endeavours undertaken by some legal commentators, predominantly from the US, to introduce new interpretations with regard to the right to self-defence in response to cyber espionage (3.2.1), and to the notion of violations of territorial sovereignty by 'cyber intrusions' (3.2.2).

3.1 Relevance of Cyber Espionage to National Security – Reloaded

Deterring foreign espionage endeavours has always been in the national interest of States. Due to new, relatively easy 'entry vectors' for (online) spies, cyber espionage seems to have escalated the respective 'threat picture': First, the effectiveness of espionage conducted by cyber means is magnified to an extreme. Second, the traditional deterrent available to targeted States, namely the possibility to prosecute and imprison caught spies, proves futile due to lack of the physical presence of intelligence agents on the target State's territory. Thus, it is since the rise of cyber espionage that a major shift in rhetoric can be perceived, however, mostly in media and scholarly writings.

Additionally, since the end of the Cold War, espionage activities have changed from politico-military to economic foci.[121] This includes the Western democracies and Allies,[122] but applies especially to less developed countries, for which economic espionage provides the technological knowledge and modern devices they could otherwise not achieve.[123] The possibilities which cyber espionage offers in terms of the speed, ease and quantity of data collection translate into escalating quantum of indirect economic loss, which is surely significant.[124] Thus, economically motivated cyber espionage is of growing concern for post-industrial, developed States,[125] as they seem particularly vulnerable to cyber espionage due to the level and sophistication of IT used.[126] In this regard some legal commentators use martial semantics, seemingly driven by ideology rather than international law proficiency. Some writers compare cyber espionage conducted during *peacetime* to 'warfare' as it 'represents an attempt to undermine the security and stability of a sovereign nation',[127] or to 'occupation',[128] thus not differentiating between the two main bodies of international law, namely law of armed conflict (LOAC) or international humanitarian law (IHL) on the one hand and

121 Sepura (n 2) 129.

122 cf Blood (n 53) 231ff (with examples and references).

123 Sepura (n 2) 134.

124 cf Centre for Strategic and International Studies, 'The Economic Impact of Cybercrime and Cyber Espionage' (Report, July 2013); O'Hara (n 57) 242.

125 Blood (n 53) 228 with further references.

126 cf Paul Cornish, 'The Economic Vulnerabilities of Developed States in a Cybered World' (Discussion Paper: The Vulnerability of the United Kingdom to Economic Cyber Warfare, Cityforum Limited, June 2011).

127 Brenner and Crescenzi (n 2) 449.

128 Melnitzky (n 61) 539 ('Chinese cyber espionage against the United States has reached such a massive scale that it more closely resembles an act of looting, which before the Internet could have only occurred coupled with military occupation, rather than series of criminal acts.').

peacetime law on the other. Lawyers also assert that economically motivated espionage would be 'the front line of a new world economic war'[129], an 'act of economic warfare'[130] or the 'newest form of warfare employed by the Chinese government [against the US]',[131] not fully appreciating the specific meaning of the term 'economic warfare', belonging to LOAC/IHL, which of applicability is triggered by a formal declaration of war, an armed conflict or occupation of a foreign territory. Admittedly, the term 'economic war' shows a broader meaning within the common language use; however, in international law it presents a term of art.

In any case, it is perceivable within scholarly writings, predominantly from the US, that cyber espionage, and especially economically motivated cyber espionage, is deemed to directly or indirectly impair the national security of the target State.[132] Due to its complexity and – in a way – reactive nature within the ever changing international security environment, the notion of national security is seldom depicted in governmental documents. The academia might offer as many definitions as there are political scientists and researchers, very probably showing many variations, reflecting the spirit of the international security situation at the time of their creation. The same applies to the term national interests, although national security strategies tend to list generic topics which are in the national interest of the respective State, e.g. economic prosperity.[133] All in all, however, it seems that the term national interests is broader than national security, entailing the latter but also including national economic security, public safety, the availability of natural resources and other vital interests.[134] It can also be claimed that the concept of vital national interests includes non-governmental economic interests of a State,[135] although the relationship to economic security, which could be seen as having a slightly different notion as national [economic] interests – however, being part of them – is not easy to delimit.

---

129 Sepura (n 2) 128.

130 Brenner and Crescenzi (n 2) 459.

131 Jonathan Eric Lewis, 'The Economic Espionage Act and the Treat of Chinese Espionage in the United States' (2008-2009) 8 Chicago-Kent Journal of Intellectual Property 189, 227.

132 Melnitzky (n 61) 538; Brenner and Crescenzi (n 2) 390-393; Georg Kerschischnig, *Cyberthreats and International Law* (Eleven International Publishing 2012) 172.

133 See e.g. Federal Republic of Germany, Federal Ministry of Defence, 'White Paper on German Security Policy and the Future of the Bundeswehr' (2006) 21 <http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/DcLBDYAgDADAWVyg_ftzC_VXsIEGaIlUXF9zhyf-lKYkcjGlijseUdbwQmgzwZCY-c4sPrpVcSlAmjiYM1xWnsbqjL1sywdHoTKR/> ('German security policy is guided by the values enshrined in the Basic Law and by the goal of safeguarding the *interests of our country*, in particular: preserving justice and freedom, democracy, security and *prosperity* for the citizens of our country and protecting them from dangers.') [emphasis added].

134 Based on: The President of the United States of America, *The Presidential Policy Directive/PPD-20* (TOP SECRET/NOFOR) 3 ('U.S. National Interests: [among others] [...] national security, [...] [and] national economic security [...]'). cf European Parliament, ECHELON report (n 87) 108: 'Since 1990, the US Administration has increasingly come to equate national security with economic security. The annual White House report entitled .National Security Strategy repeatedly emphasises that "economic security is fundamental not only to our national interests, but also to national security."').

135 Walter G Sharp, Sr, *Cyberspace and the Use of Force* (Aegis Research Corporation 1999) 131.

The notions of national security and national [economic] interests, as well as the latter's subset economic security, are certainly closely interconnected. Economic power translates, with very few exceptions,[136] into political and military power, [137] and the end of the Cold War accompanied by respective changes in geo-political relations led to the increased importance of the economic competitiveness of States. Economically motivated cyber espionage, aiming at gathering publicly unavailable or protected information on technological advances, is affecting the competitiveness of technologically advanced States. Emphasising these aspects, some commentators assert that the economic status of a State makes up a large part of its national security.[138] Going even further (and discussing Chinese espionage against US businesses), it is stated that national security is inexorably linked with the safeguarding of a State's trade secrets.[139] Such an approach understands national security as either equal[140] to national [economic] interests or, more broadly, including national [economic] interests, and leads to the peculiar consequence that any activity affecting national [economic] interests of the State targeted by industrial espionage would automatically become a matter of national security, to be discussed and decided upon within the highest circles of government.

Questions of national security and of national interest with regard to prosperity and indirect economic loss trough industrial cyber espionage need to be distinguished:

- Unauthorised copying of data containing classified information of strategic, political, economic or military nature relevant to national security; data containing intellectual property information related to the defence industry; and sensitive information related to the security of IT-systems or computer networks of critical infrastructure systems should be seen as affecting national security of a State.
- Unauthorised copying of data containing intellectual property and trade secrets of a non-defence related industry, even if the affected companies are owned by a State or where a State is a share-holder;[141] data with information on the security of IT-systems or computer networks of importance to the national economy, however, not being part of critical infrastructure; and not open-source but unclassified data of political, economic or military nature should be seen as affecting national

136 cf Paul Kennedy, *Aufstieg und Fall der großen Mächte* (Fischer 2002) *passim* (referring to Japan and Germany).

137 Brenner and Crescenzi (n 2) 394 ('In today's world a nation's economic viability is the true measure of its power.').

138 Sepura (n 2) 135.

139 Lewis (n 131) 189.

140 ibid 201.

141 eg the Land Niedersachsen has 20% shares in 'Volkswagen', and according to the *Act on the Privatization of Shares of Volkswagenwerk Gesellschaft mit beschränkter Haftung* of 21 July 1960 (so-called VW-Act) a blocking minority, which is otherwise granted by law at minimum of 25% shares. Thus, espionage against the intellectual property of Volkswagen is detrimental to Germany and other economies, however, should not be seen as affecting national security of Germany.

interests and maybe economic security, but not national security. Importantly, not each 'trade secret' of a 'national' company can be treated as a 'State secret'.

Thus, with regard to unauthorised copying of data, the situation must be assessed according to whether the information contained in the data is indeed of a national security value, or rather of a merely economic value (the latter refers to an abstract and indirect value, not to a market value).

However, a glance at media and scholarly contributions on cyber espionage, in particular with regard to the 'sabre-rattling'[142] and mutual accusations between the US, China, North Korea and Iran (although silenced after the revelations about the aforementioned alleged US mass surveillance programmes in 2013) creates the impression that the usual concepts of the enemy might be merely 'reloaded' in the cyber arena,[143] and that the traditional level of 'tolerance' of espionage might have lowered due to the enormous effectiveness of cyber espionage and the massive losses of data and confidentiality of information, being now – by trend and despite conceptual obstacles – considered a matter of national security.

3.2 Emerging Interpretations of International Law

Due to the shift in perception of cyber espionage activities as relevant to national security (as opposed to national interest), some authors, predominantly from the US, propose a re-interpretation of international law with regard to the definition of the 'use of force' pursuant to Article 2(4) UN Charter and 'armed attack' in the meaning of Article 51 of the UN Charter (3.2.1), as well as regarding the notion of violations of territorial sovereignty of a State (3.2.2).

International law is characterised by its abstractness and flexibility, allowing the system to adapt to new needs of the international community. Bearing in mind the immanent interdependence of international law and international politics, the terms 'use of force' and 'armed attack' show room for interpretation, of which the limits were explored in the past by several States aiming to accommodate their political, economic or ideological needs. The term was interpreted as including colonial and foreign domination, *apartheid*, massive and systematic human rights violations, refugee flows caused by such human rights violations, support to terrorism and the suppression of democratic movements, 'freedom fighters' and, in some (politically acceptable) cases, of peoples exercising their right to self-determination.[144] In contrast, the notion of territorial sovereignty in

142 Countless references from online media could be provided with regard to mutual accusations of these States. Due to the vast number of such reports that can easily be found on the internet, this will be omitted.

143 Supporting the impression of the 'usual concepts of enemy', see eg the report form a US based cyber security company: FireEye, 'The Advances Attack Landscape' (Report, 2013).

144 Katharina Ziolkowski, *Gerechtigkeitspostulate als Rechtfertigung von Kriegen. Zum Einfluss moderner Konzepte des Gerechten Krieges auf die völkerrechtliche Zulässigkeit zwischenstaatlicher Gewaltanwendung nach 1945* (NOMOS 2008) 208-220 and 242-246.

the context of its violations by unauthorised entrance of foreign State agents has not had a comparably turbulent history of re-interpretation endeavours. However, it currently encounters in this regard a premiere in the context of 'cyber intrusions'.

3.2.1 Cyber Espionage as Threat or Use of Force and as Armed Attack

As the author of this chapter already elaborated in the present volume [145] in detail on the interpretations of 'armed attack' (Article 51 of the UN Charter) and 'use of [armed][146] force' (Article 2(4) of the UN Charter) conducted by means of the internet or other IT-systems, it can be asserted at this stage that:

- an 'armed attack' is present in most severe cases of 'use of [armed] force' in international relations of significant scale and effects; and
- 'use of [armed] force' can be assumed if the cyber activities in question – indirectly – result in:
  - death or physical injury to living beings and/or the destruction of property, or
  - massive, medium to long-term disruption of critical infrastructure systems of a State (if in its effect equal to the physical destruction of the respective systems).

Importantly, the assessment of cyber activities as representing 'use of [armed] force' must be based on an effects-based interpretation of the term, which perfectly corresponds with the effects-based approach inherent in public international law.[147] Cyber activities can only be deemed to be violating Article 2(4) (and 51) of the UN Charter, if they – even if indirectly – result in effects comparable to the effects usually caused or intended by the employment of conventional, biological or chemical (BC) weapons. However, questions of 'use of [armed] force' and 'armed attack' on the one hand, and the topics of

145 cf idem, 'General Principles of International Law as Applicable to Cyberspace' in this volume, para 3.1.1 (on 'armed attack') and para. 3.2.1 (on 'use of [armed]force').

146 A closer examination of the norm in reference to its context within the UN Charter, to its spirit and purpose as well as to its drafting history, leads to the conclusion that 'force' in the meaning of Article 2(4) of the UN Charter means 'armed force' only. A sound interpretation of Article 2(4) of the UN Charter including aspects of its context, spirit and purpose as well as the drafting history would exceed the scope of the present analysis; *see* representatively: Randelzhofer and Dörr (n 35) 16-20. The above finding is supported by the resolutions of the UN General Assembly, which do not depict political and economic coercion as an aspect of use of 'force', but rather of the principle of non-intervention in domestic affairs of another State. See, eg, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UN GA Res 2625 [XXV] (24 October 1970) Annex, Principle 1; *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty*, UN GA Res 2131 [XX] (21 December 1965) para 2; *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, UN GA Res 36/103 (9 December 1981) para 2, principle I(b) and II (a); *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*, UN GA Res 42/22 (18 November 1987) Annex, para 8. Further, the above finding is supported by the jurisprudence of the International Court of Justice (ICJ). In its *Nicaragua Case* of 1986, the Court did not address economic coercion measures undertaken by the USA against Nicaragua as a 'use of force', but discussed it in relation to the principle of 'non-intervention', see Nicaragua (n 114) 245.

147 cf Randelzhofer and Dörr (n 35) 22.

intelligence gathering, military advantage and economic competitiveness on the other, are only seldom distinguished within the recent literature.[148]

One legal commentator points out that cyber espionage might cause much greater damage to the national security of a State *than the physical destruction* of a weapons system of a military facility.[149] Another, considering the immense scale and speed of information collection via cyberspace, claims:

> The severity of the problem of data theft is simply too great and its effects too harmful. […] The scale of theft is unprecedented. […] Prior to the Internet, looting on such a scale could only have been accomplished by a *military occupation*. The effects-based approach requirement that a cyberattack must cause damage only previously possible by traditional military force is therefore satisfied.[150]

Both opinions seem rather difficult to follow. All in all, the effects of cyber espionage, being in essence nothing but unauthorized copying of data, are not comparable to the effects caused by conventional or BC weapons, and can therefore not be deemed as 'use of [armed] force' or 'armed attack'.

One scholar proposed already in 2001 that *data and property be equated*, classifying economically motivated cyber espionage, in a second step, as 'subverting property'.[151] Although admitting that the 'purely economic nature of the actions suggests that economic espionage is an act of economic coercion and therefore is excluded from the definition of the use of force', the author, surprisingly, proposes that 'applying the consequence-based approach, an attack on a company (and by extension the company's home state) would appear to be use of force' (probably equating at this point 'subverting property' with destruction of property).[152] Although that author suggests not relying on the right to self-defence in response to such actions, he does so not for legal reasons, but rather due to political considerations, pointing out that the States responsible for economic espionage can also be Allies and trade partners.[153] This proposed view cannot be supported. The effect of economically motivated cyber espionage merely diminishes the value of the copied data and information contained therein, affecting – as the case may be – the State's economy in a very indirect and timely non-proximate way, even if the data affected symbolises economic assets. Especially, the mere copying of data is

148 eg Scott J Shackelford and Richard B Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2010-2011) 42 Georgetown Journal of International Law 971, 980.

149 Commander Todd C Huntley, 'Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare' (2010) 60 Naval Law Review 1, 39.

150 Melnitzky (n 61) 566 [emphasis by the author].

151 Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 New York University Journal of International Law & Politics 72, 89f.

152 ibid 90.

153 ibid.

not comparable to the effects of activities which usually would be considered as 'use of [armed] force' or, when showing significant scale and effects, 'armed attack' conducted by conventional or BC weapons.

Some authors suggest taking a *target-oriented approach* to the question as to whether specific cyber activities are to be deemed 'use of [armed] force' and 'armed attack'. They assert that cyber espionage should be considered as 'use of [armed] force', if information of vital interest to a State, for instance classified information, is compromised.[154] Also espionage targeting all kinds of data of military nature (regardless of the classification) is considered as 'use of [armed] force'.[155] Similarly, it is proposed to take a 'strict liability' approach according to which any cyber attack against critical national infrastructure would amount automatically to an 'armed attack' (sometimes also called a 'target-based'[156] approach).[157] Despite the uncertainty over whether mere cyber espionage activities would qualify as 'cyber attack' in the meaning of the said theory, it is claimed that '[t]rade secret data [...] has become part of our [i.e., US] critical national infrastructure.'[158] Going even further, it is affirmed that '[c]omputer espionage of a commercial nature by a state is an attack upon the vitality of [...] [commercial] infrastructure and the state as a whole'.[159] This assumed, economically motivated cyber espionage activities targeting trade or industrial secrets, as well as any data symbolising intellectual property, or the 'commercial infrastructure' would automatically amount to an armed attack and trigger the right of self-defence of the State, on which territory the affected servers are located. Interestingly, the last aspect disregards that in times of globalisation trade secrets spied upon within a State's territory can perfectly well belong to a company which is not associated with the territorial State (e.g., a foreign company using a 'cloud' offered by a local company) or to a multinational company, in which cases considerations of trade secrets being part of the 'national critical infrastructure' do not apply. As for malicious cyber activities targeting, e.g., the military sector, judging them as 'armed attacks' would lead *ad absurdum*, as, e.g., according to US officials, the US DoD systems are probed between 6- and 360-million[160] times in a day and 'successful penetrations have led to the loss of thousands of files from U.S. networks and those of

154 Joyner and Lotrionte (n 84) 846, 855; *contra*: Torsten Stein and Thilo Marauhn, 'Völkerrechtliche Aspekte von Informationsoperationen' (2000) 60 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 1, 10.

155 Joyner and Lotrionte (n 84) 846 and 856.

156 Wolfgang McGavran, 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 Tulane Journal of Technic and Intellectual Property 259, 270.

157 ibid; Eric T Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 Stanford Journal of International Law 207, 228ff and 236f; Melnitzky (n 61) 554.

158 Brenner and Crescenzi (n 2) 460f.

159 Sharp (n 135) 131.

160 Referring to the number of '6 million': Director, NSA and Commander, USCYBERCOM General Keith Alexander, 'U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM' (transcript of an address at the Center for Strategic and International Studies, 3 June 2010) <http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf>; referring to the number of '360 million': Robert Lentz, Chief Information Assurance Officer for the U.S. Department of Defense, according to Declan McCullagh, 'NSA

U.S. allies and industry partners'.[161] All in all, a target-based approach to questions of 'use of [armed] force' and 'armed attack' cannot be accepted, as this would lower the threshold for the outbreak of international armed conflict in an unacceptable way, and introduce an (additional) aspect of subjectivity into the regime of international peace and security. The presented theories seem to introduce an automatism between activities affecting national security or national [economic] interests of a State and self-defence, a construct negating international law and clearly showing the potential for extreme escalation of insecurity in international relations.

Some legal commentators view cyber espionage activities as an 'armed attack', if they demonstrate *hostile intent*, which is presumed in cases of cyber espionage targeting sensitive computer systems that are important to a State's ability to defend itself (such as early warning or military command and control systems, missile defence computer systems, and computers that maintain the safety and reliability of a nuclear stockpile).[162] In this context, cyber espionage targeting the 'commercial infrastructure collectively' is also seen as affecting the ability of a State to defend itself and therefore as a demonstration of hostile intent, invoking the victim State's right of (anticipatory) self-defence.[163] On the contrary, the assessment of the US Office of Legal Counsel of 1999 rightly states that '[…] there may be a right to use force in self defense against a single foreign electronic attack in circumstances […] *when the intruder's conduct or the context of the activity clearly manifests a malicious intent*.'[164] Herein, the decisive aspect is the *clear manifestation* of the hostile intent, which allows a reasonable assumption that a situation of an 'imminent' armed attack, triggering the right to anticipatory self-defence, is present. This will not be the case with regard to cyber espionage. First of all, cyber espionage activities will, by nature, be conducted secretly or under disguise. Even if discovered, given the challenges of attribution of online activities,[165] neither the source of the espionage activities nor the intent of the unknown or only assumed source will be accurately judged to an extent allowing the mobilisation of their own armed forces and launching of self-defence measures. Additionally, the intent of espionage as such is merely information gathering, and the aims can be perfectly non-aggressive, such as ensuring the effectiveness of the own right to self-defence or 'super-validation' of legal or political commitments of the targeted State (see section 2.1.1).

chief downplays cybersecurity power grab reports' *CNET News* (21 April 2009) <http://news.cnet.com/8301-13578_3-10224579-38.html>.

161 US Department of Defense, 'Department of Defense Strategy for Operating in Cyberspace' (July 2011) 3 <http://www.defense.gov/news/d20110714cyber.pdf >.

162 Sharp (n 135) 130.

163 ibid 131f.

164 US Department of Defense, Office of Legal Counsel, 'An Assessment of International Legal Issues in Information Operations' (May 1999) 20 <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> [emphasis added].

165 See Mauno Pihelgas, 'Back-Tracing and Anonymity in Cyberspace' in this volume.

Other authors claim that cyber espionage should be considered an 'armed attack', as such cyber activities are *indistinguishable* from those intended to cause physical damage, both requiring penetration of the targeted IT-systems or computer networks and using similar techniques like installation of 'backdoors'.[166] Additionally, it is asserted, the installation of malware in IT-systems or computer networks by a foreign State would be comparable to the entrance of military intelligence collection platforms (such as aircraft, ships or submarines) into the target State' sovereign territory, what would seem to justify self-defence, as such platforms could potentially launch (conventional) attacks.[167] Moreover, it is claimed that cyber espionage targeting 'sensitive [computer] systems that are critical to a state's vital national interests' justifies anticipatory self-defence as, due to the speed with which the penetration of a computer system can change into a destructive attack, it presents an imminent threat of an 'armed attack'.[168] As a supporting argument it is pointed out, cyber espionage would be 'much more threatening'[169] than traditional espionage, in terms of intrusiveness, greater breadth of material collection, inexpensiveness, and also the potential to result in the 'launch [of] an attack on another nation'.[170] Partly, it is asserted that additional requirements would be necessary in order to consider cyber espionage as triggering the right to (anticipatory or pre-emptive) self defence. This would be the case if, for instance, intelligence suggested that a software vulnerability would indeed be used for an imminent attack,[171] or if missile defence systems are penetrated, in connection with the discovery of the theft of 'at least a dozen passwords', if there is no sufficient time to change the 'codes' of the computer system.[172] These views are characterised by an overestimation of the speediness of a cyber manipulation and by an underestimation of the level of sophistication required to launch a cyber activity causing manipulations of and damaging effects within (and subsequently outside) IT-systems or computer networks.[173] They also ignore that cyber espionage essentially comprises of unauthorised copying of data conducted – by nature – clandestinely or under disguise, which logically leads to the conclusion that, in order to remain secret, it is not meant and will not be used to cause any detectable effects, i.e. noticeable manipulations or any harmful effects within or outside of the targeted IT-

166 Melnitzky (61) 565; Barkham (n 151) 90; similarly Anna Wortham, 'Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?' (2011-2012) 64 Federal Communications Law Journal 643, 647 and 652f (quoting at p 652 a report from the US National Research Council of 2009: 'it is often difficult to determine whether a party has been exploited or attacked'); also indirectly implying Williams (n 26) 1164 and 1185ff.

167 Melnitzky (n 61) 565, basing his legal opinion on legal deliberations of the non-lawyer and IT-scientist Dr Herbert Lin.

168 Sharp (n 135) 129f.

169 Wortham (n 166) 660.

170 ibid 658f.

171 ibid 656f.

172 Joyner and Lotrionte (n 84) 858.

173 See Markus Maybaum, 'Technical Methods, Techniques, Tools and Effects of Cyber Operations' in this volume.

system or computer network. Also, the vast quantity of material which can be obtained by the means of cyber espionage does not translate into quality of action, and certainly not into a classification as an (imminent) 'armed attack'. Importantly, the opinions presented judge the mere *possibility* of an 'armed attack' and the merely *possible* effects of a cyber intrusion as sufficient for the presence of an 'armed attack' triggering the right to (anticipatory or pre-emptive) self-defence, which is a legal assessment unsupported by international law. In order to lawfully exercise the right to self-defence a targeted State needs to either analyse the discovered malware, and discover intended, *immediately* damaging effects (something unlikely given that 'reverse engineering' of malware easily takes several months) or to wait for the effects to materialise, in case the intended or realised effects indeed correspond to the notion of an 'armed attack' in the meaning of Article 51 of the UN Charter.[174] Any other reaction would violate international law and, considering the challenges of attribution of online activities, bear the risk of misinterpretation of the danger and of 'striking back at the wrong party and [commencing or] escalating hostilities'.[175]

Some legal commentators consider cyber espionage as a forbidden *threat of [armed] force* in the meaning of Article 2(4) of the UN Charter because there would be no possibility of ascertaining the non-aggressive intent of the attacking party.[176] However, a 'threat of force' requires a coercive intent directed towards a specific behaviour on the part of the other State.[177] Mere information collecting by cyber means will not fulfil this requirement. However, cyber espionage can be viewed as a preparation activity. Such activities do imply a threat of force against any possible aggressor, but are undertaken under the umbrella of and in conformity with the right to self-defence.[178] A distinction between offensive and defensive preparations is often impossible.[179] Thus, uncertainty as to the offensive or defensive intent of specific cyber espionage activities, which are widely considered as supporting or ensuring self-defence possibilities of a spying State, does not justify assuming the presence of the illegal 'threat of [armed] force'.

In conclusion, cyber espionage cannot be deemed either a 'threat' or 'use of [armed] force' in the meaning of Article 2(4) of the UN Charter, nor an 'armed attack' pursuant to Article 51 of the UN Charter.[180] It shall be mentioned that, as espionage *per se* is

174 So also Huntley (n 149) 36.

175 ibid (quoting US National Research Council report of 2009).

176 Wortham (n 166) 656.

177 Randelzhofer and Dörr (n 35) 43.

178 ibid 42.

179 ibid.

180 Anthony D'Amato, 'International Law, Cybernetics, and Cyberspace', in Michael N Schmitt & Brian T O'Donnell (eds), *Computer Network Attack and International Law* (Newport / Rhode Island, US Naval War College, 2002) 59–71, 67; Stein and Marauhn (n 154) 32 with further references; Wolff Heintschel von Heinegg, 'Informationskrieg und Völkerrecht. Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung', in Volker Epping, Horst Fischer & Wolff Heintschel

not illegal under international law, and therefore not an internationally wrongful act, the conduct of so-called countermeasures in response to cyber espionage, as discussed within the US literature,[181] would be illegal (see Article 49(1) of the ILC *Draft Articles on Responsibility of States for Internationally Wrongful Acts*)[182]. The instruments for counter-action available to States during peacetime are political, economic and diplomatic means.

3.2.2 Cyber Espionage as Violation of Territorial Sovereignty

Espionage conducted within another State's sovereign areas – i.e., the land territory, internal waters, territorial sea, archipelagic waters, national airspace or on platforms (e.g., vessels, aircraft or satellites) – traditionally requires the clandestine and unauthorised entry of a foreign State's organ, agent etc. or of an information collecting platform, such as an aircraft, a vessel or submarine. In such cases the respective State's territorial sovereignty, i.e., the exercise of full and *exclusive* authority over a territory or area,[183] would be violated. As the PCIJ stated in the *Lotus* case '[...] the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State.'[184] Thus, an unauthorised entry into, and presence in, a sovereign area of a State by a foreign organ, agent etc. (acting in official capacity in a foreign sovereign area) or of an intelligence collecting platform would violate the territorial sovereignty of that State.[185]

Thus, both traditional and cyber espionage, the latter if requiring the so-called 'close access' to, e.g., air gapped IT-systems or computer networks, would be accompanied by a violation of the territorial sovereignty of the target State if conducted by or otherwise attributable to a foreign State. E.g., undersea fibre cable tapping, requiring either cutting and introducing a specific device or physically bending a cable, which is reportedly[186] done within the UK (and US) espionage program named 'Tempora', collecting around 21 million gigabytes of data per day, would violate the territorial sovereignty of another State only if conducted within the territorial sea or on the land territory of that State.

---

von Heinegg (eds), *Brücken bauen und begehen. Festschrift für Knut Ipsen zum 65. Geburtstag* (CH Beck 2000) 134.

181 eg Brenner and Crescenzi (n 2) 454.

182 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UNGA Res 56/83 (12 December 2001) annex.

183 Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012) 7ff, 10, 13.

184 Lotus case (n 118) 18.

185 Chesterman (n 66) 1082.

186 Olga Khazan, 'The Creepy, Long-Standing Practice of Undersea Cable Tapping' *The Atlantic* (16 July 2013) <http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>.

Such activities conducted on the high seas would not violate the territorial sovereignty of any State, but could be in violation of certain norms of the law of the sea.[187]

With regard to cyber activities conducted remotely, i.e. not requiring the physical presence in the targeted State's sovereign areas, it can be deemed as acknowledged that any cyber activity causing a perceivable *physical* effect in another State's sovereign area would violate the territorial sovereignty of that State.[188] However, cyber espionage is meant to remain a secret activity, thus logically should not cause any perceivable physical effect. It is questionable whether a mere 'unauthorised virtual trespass' would be comparable to a physical entry or presence into a foreign territory. A US DoD legal memo of 1999 stated:

> An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, *but such issues have yet to be addressed in the international community*.[189]

Over a decade later, the question still remains open – perfectly consistent with the 'policy of silence' within the international community of States with regard to matters of espionage.

It is doubtful whether an unauthorised 'virtual trespass' of or 'virtual presence' in an IT-system or computer network that runs on servers located in the sovereign area of another State can be equated with a physical presence of a spying State organ, agent etc. or a platform.[190] Essentially, cyber espionage consists of unauthorised copying of data and of necessary adjunctive activities, i.e., amendments of data to obtain access to the IT-systems and cover the traces of any espionage activity. Those data amendments, such as

- modification of data (e.g., access lists or rules) or exploitation of a system vulnerability in order to obtain access to the IT-systems or computer networks,
- modifications of data, including deleting, e.g. of event log messages of the targeted IT-system or computer network, aiming at covering the traces of the intruder's own espionage activities,

187 On undersea cable protection see Wolff Heintschel von Heinegg, 'Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law' in this volume.

188 cf Heintschel von Heinegg (n 183) 11ff, 16; Lawrence T Greenberg, Seymour E Goodman and Kevin J Soo Hoo, *Information Warfare and International Law* (U.S. National Defence University 1998) 24; similar: Joyner and Lotrionte (n 84) 843.

189 US Department of Defense, Office of General Counsel (n 164) 19f [emphasis added].

190 Generally agreeing: Forcese (n 26) 208, Heintschel von Heinegg (n 183) 11.

- modifications of data, including saving data, on the targeted IT-systems or computer networks, e.g., installation of Remote Access Tools (RATs) and other software as necessary for current or further espionage activities

are – in some cases – inevitable means in order to be able to copy the targeted data. However, these data amendments do not cause any further, i.e. secondary, tertiary etc., *physical*[191] effects in a foreign State's sovereign area (in order to ensure the secrecy of the operation).

At first sight, it would be, though, conceivable, to compare the use of cyber infrastructure as a 'platform' for spying with the use of traditional information collecting 'platforms' such as State aircraft, vessels, or submarines intruding into the sovereign area of the target State. However, in the case of cyber espionage, the 'platform' used for espionage, namely the target IT-system or computer network, is already located in the target State's sovereign area and an intrusion by another 'IT-platform' from outside the borders is not present. Also, the fact that cyber espionage activities – as opposed to satellite and other remote surveillance techniques focusing targets in another State's sovereign area – nowadays need to 'intrude' by overcoming technical barriers, such as firewalls, does not justify another assessment.

However, as one author rightly remarked, it could be argued that an intrusion into the cyber infrastructure of a State by another State's organs, agents etc. is considered an 'exercise of jurisdiction on foreign territory that always constitutes a violation of the principle of territorial sovereignty'.[192] This view focuses not on the 'virtual trespass' but on the 'exercise of authority' by a representative of a foreign State. (There are indications that such a view is currently taken by the US administration.[193]) It is only in this sense that 'cyber intrusions' by foreign State organs, agents etc. could be considered to be a violation of the territorial sovereignty of the target State.

4. International Law Policy Considerations

About 15 years ago, the scholarly discourse on malicious cyber activities centred around the distinction between illegal 'use of [armed] force' and 'armed attack', and perfectly legal political or economic 'coercion'. [194] The discussion was driven by the tendency

191 An IT-expert can perceive changes in, eg, the log-files of a system he or she administers as being 'physically perceivable'. However, this approach cannot be applied to public international law that, in this regard, is rather 'simplistic', focusing on clearly perceivable effects which can be dealt with on the level of international relations.

192 Heintschel von Heinegg, ibid 12.

193 The President of the United States of America, *International Strategy for Cyberspace* (May 2011) 12ff (asserting the right to respond to 'exploitation of networks' with all necessary means, including use of force, as the case may be).

194 See eg Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law (3) 914ff; idem, 'Cyber Operations and the *Jus Ad Bellum* Revised' (2011) 56 Villanova Law Review 576ff; Barkham (n 151) 58 and 84ff.

to define the threshold of 'use of [armed] force' as relatively high, thus leaving – in legal terms – more manoeuvring room for coercion activities of a political or economic nature. Recent writings on malicious cyber activities focus on the distinction between the illegal 'armed attack' and the – in terms of international law – not illegal espionage activities of States, showing a tendency to equate them.

Competing interpretations of the terms 'use of [armed] force' and 'armed attack' have always reflected certain distributions of power.[195] Historically, the prevailing interpretations, namely excluding political and economic coercion,[196] were especially connected to the satisfaction with the political *status quo* as perceived during the negations of the UN Charter in 1945.[197] During this time, and over the following decades, the Great Powers had a strategic advantage in terms of their possibilities of political and economic coercion, and the argumentation lines of many legal commentators focused on maintaining those possibilities in legal terms, and also in the cyber context.

The recently perceivable shift in the focus of analysis and of the lines of juridical argumentation might be based on the notion that the satisfaction with the political *status quo* has very probably changed with regard to cyber espionage. In contrast to the circumstances accompanying the discourse on political or economic coercion, economically and militarily strong States are those which have far more to lose, especially through economically motivated cyber espionage targeting their industrial and post-industrial technological achievements, impairing their competitive lead, and subsequently reducing their advantageous standing within the globalised world economy system. Hereby, the high standard of their own economic development as well as the level and sophistication of the IT used present a strategic disadvantage to the post-industrial, developed States. The asymmetric advantage offered by cyber means has the potential to negate much of those States' conventional power.[198] Notably, the distribution of such power is not reflected by the distribution of the global cyber power.[199] The interpretational efforts aiming to outlaw politically and economically motivated cyber espionage as illegal 'use of [armed] force' or 'armed attack' (see section 3.2.1) or as a violation of the territorial sovereignty of the targeted State (see section 3.2.2), can be deemed to be endeavours to preserve the strategic advantages of the Great Powers. However, lowering the threshold of Articles 2(4) and 51 of the UN Charter to include cyber espionage is not desirable as it 'may introduce greater security instability

195 Matthew C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale Journal of International Law 421, 448.

196 During the negotiations of Art 2(4) of the UN Charter, some developing as well as socialistic States endeavoured to include economic (as well as political) coercion within the prohibition of 'use of force'. These efforts were not successful. See B.E. Carter, 'Economic Coercion' in MPEPIL (n 43) MN 6. On UN GA Resolution practice and international jurisprudence see n 146.

197 Waxman (n 195) 449.

198 cf also Huntley (n 149) 33.

199 cf similarly Waxman (n 195) 450.

to the international system by eroding normative constrains on military responses to nonmilitary harms'.[200] In the end, and regardless of all the dogmatic obstacles mentioned, the interpretations presented above can be deemed unrealistic, as the Great Powers will not seek to deprive themselves, in legal terms, of the highly effective, secure, relatively swift and inexpensive means of intelligence gathering which cyber espionage offers.

Furthermore, as the vast majority of legal commentators advocating outlawing of (economically motivated) cyber espionage as 'use of [armed] force', 'armed attack' or as violations of the territorial sovereignty of the target State are either active or retired US government service members, a short glance at the US policy on the matter seems appropriate. The US *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* [201] of February 2013, states: 'Trade secret theft threatens American businesses, undermines national security, and places the security of the U.S. economy in jeopardy.' [202] However, the strategy, being an inter-agency[203] effort, including the DoD and the Department of Homeland Security, does not contain any notion of deterrence, but foresees as 'strategy action items':

(1) increasing diplomatic engagement to protect trade secrets overseas;
(2) promoting voluntary best practices by private industry to protect trade secrets;
(3) enhancing domestic law enforcement operations;
(4) improving domestic legislation (in regard to national law enforcement); and
(5) increasing public awareness and stakeholder outreach.

The strategy mentions cyber espionage not in the context of military or homeland security, but as an issue of domestic law enforcement.[204] Accordingly, responsibility for cyber crime and intellectual property crime rests within one Department of Justice's unit, the Computer Crime and Intellectual Property Section. It 'is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide.'[205] Some authors warn that the strategy is ill-

200 also: ibid 454.

201 Executive Office of the President of the United States, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (February 2013) <http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>.

202 ibid 1 [emphasis added].

203 ibid (Acknowledgements) ('product of a collaborative effort and reflects the recommendations and input from various entities of the U.S. government, including the Departments of Commerce, Defense, Homeland Security, Justice, State, Treasury, the Office of the Director of National Intelligence and the Office of the United States Trade Representative').

204 ibid 7 ('The Department of Justice has made the investigation and prosecution of corporate and state sponsored trade secret theft a top priority. The Department of Justice and the FBI will continue to prioritize these investigations and prosecutions and focus law enforcement efforts on combating trade secret theft. The FBI is also expanding its efforts to fight computer intrusions that involve the theft of trade secrets by individual, corporate, and nation-state cyber hackers.').

205 US Department of Justice, website 'Computer Crime and Intellectual Property Section' <http://www.justice.gov/criminal/cybercrime/>.

suited to addressing the problem of cyber espionage, foreseeing a deteriorating political climate and an increase in espionage in the future.[206] However, this strategy not only correctly reflects the current state of international law, but also shows the unwillingness of the US to outlaw (politically or economically motivated) espionage. In general terms, all States have an interest in espionage activities, and State practice is to be expected to remain constant in this matter.

With regard to any potential endeavours of outlawing industrial espionage (or in terms of popular science: 'trade secret theft'), the WTO seems to be the appropriate forum. Only when outlawed in legal terms, States will have the option to undertake legal remedies (that international law offers in cases of its violation) against unauthorised copying of data symbolising 'intellectual property' or trade secrets, such as countermeasures or recourse to international courts, tribunals or (WTO) decision bodies. However, States already have at their disposal instruments of 'soft power' for counter-action, such as economic, political and diplomatic means.

In any case, declaring cyber espionage to be a 'use of [armed] force' or 'armed attack' does not show potential for producing a meaningful decrease of or protective effect against cyber espionage. It is understandable that States seek to find an alternative for the traditional deterrent against espionage, namely the penalisation of espionage activities within national law and the prospect of prosecution and imprisonment of caught spies; a futile aspiration with regard to remotely conducted cyber espionage. However, military action will neither diminish the cyber espionage potential, nor will corresponding announcements have a deterrent effect, as deterrence hardly works in cases of hidden and secretly operating eavesdropping software and against anonymous actors. The only way forward is to improve cyber security and resilience of the own IT-systems or computer networks. Notably, it is in this sense that many of the national cyber security strategies[207] list cyber espionage as one of the cyber threats to counter.

5. Conclusions

Peacetime espionage is as old as mankind. On the international law level, neither its legality nor its illegality can be established. Thus, peacetime espionage conducted by States is either permitted because it is not forbidden (based on the notion of State sovereignty), or it is not regulated and therefore not justiciable under international law (*non liquet* based on consensual approach to international law). In consequence, States are – in general, and apart from a few specific limitations – free to conduct peacetime espionage activities, by whatever means they choose.

206 Fidler (n 56).

207 See list at NATO CCD COE, National Strategies & Policies <http://ccdcoe.org/328.html>.

Preclusion of espionage endeavours of foreign States has always been in the national interest of the target State. Cyber espionage, however, seems to have escalated the threat picture. Due to new, relatively easy 'entry vectors' for (online) spies and the vast amount of data that can be copied in only a few minutes, the effectiveness of espionage conducted by cyber means is magnified to an extreme. At the same time, the traditional deterrent that targeted States have at their disposal – namely the possibility to prosecute and imprison caught spies – proves futile due to lack of physical presence of intelligence personnel on the target State's territory in cases of remote activities. Additionally, since the end of the Cold War, espionage activities have changed from a politico-military to an economic focus. The swiftness and relative easiness of cyber espionage and the vast amount of data to be collected by its means translates into an escalating quantum of economic loss. Accordingly, not only martial semantics referring to 'economic warfare' are seen in media and scholarly writings, but also a general shift in the perception of cyber espionage as a threat affecting national security, as opposed to national [economic] interests (or the subset economic security).

Hence, some legal commentators propose to reinterpret international law to outlaw cyber espionage as a 'threat' or 'use of [armed] force' pursuant to Article 2(4) UN Charter and an 'armed attack' according to Article 51 UN Charter, or as a violation of the territorial sovereignty of the target State. The different approaches and arguments brought forward cannot be supported, as they are based on concepts negating the international law system and its inherent effects-based approach, or would introduce greater security instability in international relations, or both. With regard to 'cyber intrusions' into IT-systems or computer networks physically located on another State's territory or area under its exclusive jurisdiction, a violation of the territorial sovereignty of the target State is thinkable in terms of an 'exercise of jurisdiction' by a representative of a foreign State (but not the mere 'virtual trespass').

The new tendencies in public international law as presented can be seen to reflect changes in the political *status quo* as introduced by the cyber era. Particularly the traditional and recognised core interpretations of 'use of [armed] force' and 'armed attack' reflected the distribution of conventional power of economically and militarily strong States, excluding, e.g., political and economic coercion from the respective prohibitions. Cyber espionage changed the picture, as post-industrial, developed States are especially vulnerable to cyber espionage due to the level and sophistication of the IT used, and because they have far more to lose in terms of technological advance and competitive lead on the global market. Cyber power is not mirroring the distribution of traditional power. The proposed re-interpretations of public international law can be deemed as endeavours to preserve the traditional strategic advantages of the Great Powers. In this regard, it can be only warned of 'aligning legal interpretations with strategic interests

[as it] is exceptionally difficult because the future effects of information technology on power [...] remain so uncertain.'[208]

Military action will neither diminish the cyber espionage potential, nor will corresponding announcements have a deterring impact, as deterrence hardly works in cases of hidden and secretly operating eavesdropping software and against anonymous actors. In response to foreign cyber espionage, States should make use of the remedies currently at their disposal; diplomatic, economic and political means. In the end, outlawing espionage, conducted by whatever means, seems illusory as States will not want to deprive themselves of this tool. The only way to counter the threat of foreign States' cyber espionage is to improve the cyber security and resilience of the own IT-systems or computer networks, as envisioned by a multitude of national cyber security strategies.

[208] Waxman (n 195) 425.

Thilo Marauhn

Customary Rules of International Environmental Law - Can they Provide Guidance for Developing a Peacetime Regime for Cyberspace?

1. An Environmental Perception of Cyberspace

In its 1996 Nuclear Weapons Advisory Opinion the International Court of Justice (ICJ) stated that the 'environment is not an abstraction but represents the living space, the quality of life and the very health of human beings, including generations unborn'.[1] The European Commission, when presenting a draft Council resolution on the continuation and implementation of a European Community Policy and Action Programme on the Environment in 1976, used the term 'environment' to 'cover all those elements which in their complex inter-relationships form the framework, setting and living conditions for mankind, by their very existence or by virtue of their impact'.[2] Typically, definitions or descriptions of the environment refer to place, time and, in the context of protecting the environment, sources of potential pollution.[3] Increasingly, they take a 'multi-media' approach,[4] aiming at comprehensive coverage of the environment and also focusing on ecological aspects. The 1992 *Helsinki Transboundary Watercourses Convention*[5] includes as part of transboundary impact a broad variety of effects on the environment, such as 'effects on human health and safety, flora, fauna, soil, air water, climate, landscape and historical monuments or other physical structures or the interaction among these factors, [...] effects on the cultural heritage or socio-economic conditions'.[6] The 1993 *Convention on Civil Liability for Damage Resulting from Activities Dangerous to the Environment,*[7] concluded within the framework of the Council of Europe, defines environment in Article 2(10) as including 'natural resources both abiotic and biotic, such as air, water, soil, fauna and flora and the interaction between the same factors; property which forms part of the cultural heritage; and the characteristic aspects of the landscape'. Irrespective of their entry into force, it can be taken that various treaties and other instruments of international environmental law primarily address the environment, even though this is 'a term everyone understands

1 ICJ, *Legality of the Threat or Use of Nuclear Weapons [Advisory Opinion]* [1996] ICJ Rep 226, 241.

2 EEC OJ C 115/2 of 24 May 1976.

3 See, among others, M.-L. Larsson, Legal Definitions of the Environment and of Environmental Damage, [1999] Scandinavian Studies in Law 38, 155, at 157-158.

4 *Ibid*., at 172.

5 *Convention on the Protection and Use of Transboundary Watercourses and International Lakes*, 1936, UNTS, 269.

6 *Ibid*., Article 1, para. 2.

7 ETS no. 150.

and no one is able satisfactorily to define'[8] from an anthropocentric perspective (i.e. focusing on the human environment), and in this context is typically taken in its most comprehensive sense, including at least physical and socio-economic factors. While some complain that the 'boundaries of what constitutes an "environmental" issue have already become blurred',[9] this can be taken as a reference to the interconnectedness of factors external to but impacting on the human being.

Based on this approach to the environment, cyberspace does not seem to be that different, at least not from a lawyer's perspective. For the purposes of this chapter and based upon research conducted by NATO's Cooperative Cyber Defence Centre of Excellence, cyberspace is understood to be 'a global, non-physical, conceptual space, which includes physical and technical components, i.e., the internet, the "global public memory" contained on publicly accessible websites, as well as all entities and individuals connected to the internet'.[10] It has 'political, economic, social and cultural aspects going far beyond the notion of a pure means of information transfer'.[11] It is contended here that, even though the term 'cyberspace' suggests the possibility of spatial definition, cyberspace can as much and as little be spatially defined as the environment.

Rather than defining the extent of the environment, humans operate within the environment, are affected by the environment, make use of it, and affect the environment by their activities. The environment may be State territory; it may be areas beyond national jurisdiction; it may be national and international. Dan Bodansky has raised the question, '[w]hat makes an environmental issue international?'[12] He has first identified transboundary environmental problems and global commons problems, characterised by 'physical spillovers'.[13] Other problems have been framed by him in terms of 'economic spillovers',[14] pointing out that 'one country can have a substantial effect on the environment of another country, not only through physical pollution, but also through investment and trade'.[15] Beyond these, Bodansky argues, there may be cases, which are international 'only because the international community has taken [them] up as such'.[16]

---

8 D. Bodansky, *The Art and Craft of International Environmental Law* (Harvard University Press 2010), at 9-10 takes up this phrase, referring to L.K. Caldwell, *International Environmental Policy: Emergence and Dimensions* (2nd ed, Duke University Press 1990), at 197 (who, however, refers to the term development in this context).

9 *Ibid*., at 11.

10 K. Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications* (NATO CCD COE Publication 2013), at 5.

11 *Ibid*., at 5.

12 Bodansky (note 8), at 11.

13 *Ibid*., at 11.

14 *Ibid*., at 11.

15 *Ibid*., at 12.

16 *Ibid*., at 12, referring to the protection of the panda and its habitat. It is noteworthy that Bodansky distinguishes global environmental law (which he rather perceives as being the result of comparative environmental law and

It may thus be argued that indeed there are already parallels between the environment and cyberspace, from a definitional perspective. More parallels arise when considering each of them from a functional perspective. The environment provides natural resources[17] which are useful and valuable to mankind. Parts of it can thus be perceived as a transboundary resource (such as transboundary watercourses),[18] others as a global resource (including the climate, the ozone, and the oceans).[19] Accordingly, environmental and international environmental law can also be framed as natural resources and international natural resource law.[20] Similarly, cyberspace is a resource which mankind can make use of and exploit. Cyberspace-based communications are indispensable for socio-economic relations, and cyberspace more generally offers further potential for a broad variety of economic activities.[21]

Considering both the environment and cyberspace as a resource opens a further perspective on parallels. The two resources are not free: their access and usage entails costs and, since neither is unlimited, their sustainable management and preservation also requires funding. Costs are not necessarily borne by those who cause them; thus, both the natural environment and cyberspace have to address the problem of internalising external costs.[22]

While there are parallels between the two subjects, there are also differences. There are ecocentric approaches to environmental protection[23] which cyberspace cannot parallel. Cyberspace is not part of the natural environment, but is a technical environment which

being built upon convergence of national environmental laws) from international environmental law (*Ibid*., at 12-13).

17 The World Commission on Environment and Development in its Report 'Our Common Future' (1987) referred to natural resources as 'plants, animals, and micro-organisms, and the non-living elements of the environment on which they depend' (*Ibid*., at 149).

18 For a discussion of pertinent treaty law see Ulrich Beyerlin and Vanessa Holzer, 'Conservation of Natural Resources', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2009), at paras. 24-31 (accessed on 30/10/2013).

19 It is noteworthy that these 'resources' are not addressed in the above-mentioned contribution on the conservation of natural resources by Beyerlin and Holzer (note 18) but by Ulrich Beyerlin andand Jenny Grote, 'Stoutenburg, Environment, International Protection', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2010), at paras. 30-37 and paras. 48-56 even though they explicitly refer to marine resources (*Ibid*., at paras. 49-51) (accessed on 30/10/2013).

20 For a broad perspective see the recently published volume by Elena Merino Blanco and Jona Razzaque, *Globalisation and Natural Resources Law: Challenges, Key Issues and Perspectives* (Edward Elgar 2011), *passim*.

21 On the economics of cyberspace see N. Elkin-Koren and E.M. Salzberger, *Law, Economics and Cyberspace. The Effects of Cyberspace on the Economic Analysis of Law* (Edward Elgar 2004), *passim*. For a discussion of the economics of cyber security see T. Moore, 'Introducing the Economics of Cybersecurity: Principles and Policy Options, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy' (2010), paper available at <http://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf> (accessed on 30/10/2013).

22 For a discussion in the environmental context and for a modelled approach see T. Kosugia, K. Tokimatsub, A. Kurosawab, N. Itsuboc, H. Yagitad and M. Sakagamie, Internalization of the External Costs of Global Environmental Damage in an Integrated Assessment Model, [2009], Energy Policy 37, 2664-2678.

23 B. Donnelly and P. Bishop, Natural Law and Ecocentrism, [2007] Journal of Environmental Law 19, 89-101.

makes use of certain geophysical and other naturally available properties. Cyberspace is largely man-made, whereas the natural environment has not been created by man; nature is the subject of discovery, whereas cyberspace is the outcome of creativity. There are more parallels and differences than can be pointed out in the introductory part of this short chapter, and their identification and discussion is not the subject to be addressed here. Rather, the existence of such parallels gives rise to the question as to what extent future regulation of cyberspace can build upon the already existing regulation of the international environment. This chapter will provide insights into possible future regulation of cyberspace from the perspective of international environmental law.

Before entering into a more detailed discussion of the customary rules of international environmental law which may be of use when addressing cyberspace, some caveats must be made. First, international environmental law does not regulate the environment but, more precisely, it regulates human behaviour relevant for the environment. Second, while all legal rules are designed to be applied to facts,[24] the application of environmental law to the facts, and particularly of international environmental law, is more complex than the application of the law in respect of other subject matters. Third, this complexity is partly due to the amount of scientific uncertainty.[25]

It is useful first to take stock of and look at the sources of international environmental law. This paves the way for a discussion of selected key concepts of international environmental law. These include the obligation not to cause harm, the precautionary approach, the 'polluter pays' concept, the notion of sustainable development and the common heritage approach. The fourth part of this chapter will raise the question of the transferability of such key concepts to the regulation of cyberspace, and the relationship between *lex lata* and *lex ferenda*. The conclusions will summarise this chapter's findings and develop regulatory perspectives for the peacetime use of cyberspace.

2. Taking Stock: Sources of International Environmental Law

The main body of today's international environmental law has been developed since 1972,[26] when States got together at Stockholm for the purpose of the United Nations (UN) Conference on the Human Environment.[27] Only a few agreements go back earlier, and these largely took a utilitarian approach.[28] However, one of the most important

24 As stated by F. Rigaux, 'The Concept of Fact in Legal Science', in: P. Nerhot (ed.), *Law, Interpretation and Reality* (Springer 1990), 38, at 48, 'fact and law do not belong to two different worlds as if fact occupied the earthly space of crude factuality and law was accommodated in a celestial universe of pure normativity'.

25 J.E. Viñuales, 'Legal Techniques for Dealing with Scientific Uncertainty in Environmental Law', [2010] Vanderbilt Journal of Transnational Law 43, 437-503.

26 For an account of the history of international environmental law see U. Beyerlin and T. Marauhn, *International Environmental Law* (Hart 2011), at 1-30.

27 See the *Report of the UN Conference on the Human Environment*, Stockholm UN Doc A/CONF48/14/Rev1.

28 Beyerlin and Marauhn (note 26), at 3.

rules of international environmental law, the obligation to prevent transboundary environmental harm or to minimise the risk thereof,[29] was already established by the arbitral tribunal in the *Trail Smelter* case in 1941.[30] This rule was later confirmed by Principle 21 of the *Stockholm Declaration*[31] and Principle 2 of the *Rio Declaration,*[32] as well as by international courts and tribunals.[33]

Most of today's international environmental law is treaty-based.[34] One of the reasons for primarily making use of treaties is 'their capacity to solve a given environmental problem as definitely and thoroughly as possible'.[35] Furthermore, treaties allow for rational approaches,[36] they provide more legal certainty than non-treaty sources,[37] and 'they allow states to tailor a regime's institutional arrangements and mechanisms to fit the particular problem'.[38] The treaty-making techniques most commonly applied in international environmental law allow for 'dynamic arrangements, establishing ongoing regulatory processes'.[39] Most prominent are the 'framework convention and protocol'[40] and the 'convention and annexes' approaches.[41] The first of these is a two-step approach involving the conclusion of an international framework convention, which is typically broadly worded, and the subsequent elaboration of one or more subsequent protocols; the framework convention operates as a 'road map'[42] for the future regulatory process. The second approach has over time even involved a delegation of the power to adopt

29 On the concept of no harm see Beyerlin and Marauhn, *Ibid*., at 39-46; and in this volume B. Pirker, Territorial Sovereignty and Integrity and the Challenges of Cyberspace (2013).

30 *The Trail Smelter Arbitration Case (Decision of 11 March 1941) (United States v Canada)* (1941) 3 RIAA 1938; for a discussion see R.A. Miller, 'Trail Smelter Arbitration', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2007).

31 See Report (note 27), 3 *et seq*.

32 *Report of the United Nations Conference on Environment and Development* (3–14 June 1992) UN Doc A/CONF.151/26/Rev.1 (Vol. I), at 3 *et seq*.

33 See, among others, Beyerlin and Marauhn (note 26), at 39-40 with further references.

34 Beyerlin and Marauhn (note 26), at 265: 'International treaties are the most frequently used source of international law in international environmental relations'. Similarly, Bodansky (note 8), at 154: 'From the inception of international environmental law, treaties and other forms of negotiated agreements have been the predominant means of achieving international cooperation'. For a broader perspective see T. Gehring, Treaty-Making and Treaty Evolution, in D. Bodansky, J. Brunnée and E. Hey (eds.), *The Oxford Handbook of International Environmental Law* (Oxford 2007), 467, at 469-473.

35 Beyerlin and Marauhn (note 26), at 265, arguing that 'international treaties are by far superior to customary international law which, by its very nature, remains rather abstract in substance'.

36 Bodansky (note 8), at 154.

37 *Ibid*., at 154.

38 *Ibid*., at 154.

39 *Ibid*., at 155.

40 Beyerlin and Marauhn (note 26), at 270-272. On the dynamics of these processes see also Gehring (note 34), at 485-495.

41 *Ibid*., at 272-273.

42 *Ibid*., at 271.

technical annexes to the Conferences of Parties[43] typically established as part of multilateral environmental agreements.

While treaties indeed offer the possibility of designing tailor-made agreements to meet particular environmental problems and at the same time not asking too much of States, they are not without problems for international environmental law as a whole, since they contribute to what has rightly been labelled the fragmentation of international environmental law.[44]

Customary international environmental law does not contribute to fragmentation but neither does it promote the constitutionalisation of international environmental law.[45] The existing customary elements of international environmental law are largely framed in general rules. As Dupuy pointed out, 'customary international environmental law is both omnipresent and of paramount importance'.[46] At the same time, Dupuy highlights the dilemma that it is difficult to prove the existence of particular rules of international environmental law and that scholarly argument often 'cannot in itself furnish proof or undeniable evidence capable of convincing states of the existence of a binding obligation'.[47] He argues that 'the law-making process in the field of customary international environmental law should not be arbitrarily disconnected from its ecological and political stakes'.[48] Some scholars are rather sceptical about the existence of any customary rules of international environmental law, or at least of proving their existence in light of the difficulty in proving States' *opinio iuris*.[49] It is against this background that the function of the rules of customary international environmental law have been described as 'filling lacunae which often arise in situations where a certain question has been left unsolved by the treaty regulation concerned or in the relationship between States, which are partly bound, partly not bound by a certain treaty'.[50]

In sum, today's international environmental law is a complex composition of treaty-based and customary international law rules. These rules cover a broad range of issues, from freshwater resources, through oceans and marine resources, air, ozone, and climate, flora, fauna and biological diversity, to waste and hazardous substances. Whether any of these rules can as such be applied to cyberspace depends on the extent to which the various environmental goods or values protected are directly or indirectly

43 See G. Ulfstein, Treaty Bodies, in: Bodansky, Brunnée andand Hey (note 34), 877, at 879-881.

44 Gehring (note 34), at 475-476, focusing in particular on institutional fragmentation of international environmental law.

45 See the discussion on constitutionalisation in international environmental law by Gehring, *Ibid*., at 473-475.

46 P.-M. Dupuy, Formation of Customary International Law and General Principles, in: Bodansky, Brunnée andand Hey (note 34), 449, at 453.

47 *Ibid*., at 453.

48 *Ibid*., at 453.

49 See Bodansky (note 8), at 197-199, raising the question 'Are International Environmental Norms Customary in Nature?' (*Ibid*., at 197).

50 Beyerlin and Marauhn (note 26), at 282.

affected. Much more promising than directly relying upon international environmental law to regulate cyberspace is the option of obtaining guidance from what will be discussed below; key concepts of international environmental law and their meaning for cyberspace. Just as customary international law can fill in gaps, it was very useful in the early stages of developing international environmental law, providing overall guidance for a relatively new area of public international law.

3. The Meaning of Selected Key Concepts of International Environmental Law for Cyberspace

Many documents adopted by States in the context of efforts to protect or regulate the environment include what are labelled 'principles'. This is true for the 1992 *Rio Declaration* which expressly lays down a catalogue of 27 principles, including the obligation of States 'to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction' (Principle 2), and basic concepts on sustainable development (Principles 1, 4, 5, 6, 8 and 12), precautionary action (Principle 15) and that the polluter should pay (Principle 16). Neither does the *Rio Declaration* pretend to establish binding rules nor have commentators, in general, derived from the *Declaration* any legally binding obligations. Indeed, as such, the *Declaration* is not legally binding, although this does not exclude that some of the principles actually restate or have emerged into rules of customary international law. In order to avoid any misperceptions about their respective legal status, the following discussion of 'key concepts' will not label these as 'principles' or 'rules' as separated by Dworkin's legal theory.[51] According to Dworkin, policies stipulate political ideals, and only principles and rules enjoy normative quality: rules aim to make addressees take action; principles only provide guidance to the addressees on future rule-making and decision-making processes. In other words, 'rules create obligations of conduct, [and] […] of result',[52] setting out 'legal consequences that follow automatically when the conditions provided are met',[53] whereas principles 'do not prescribe or proscribe a particular state behaviour',[54] but aim to influence decision-making processes and the interpretation of rules.[55] For the purpose of explaining these concepts and identifying their potential for the regulation of cyberspace, the notion of a 'key concept' will be applied, with its impact on State behaviour being of a different normative quality.[56]

51 R. Dworkin, *Taking Rights Seriously* (Bloomsbury 1977), at 22.

52 Beyerlin and Marauhn (note 26), at 37.

53 Dworkin (note 51), at 25.

54 Beyerlin and Marauhn (note 26), at 37.

55 U. Beyerlin, Different Types of Norms in International Environmental Law: Policies, Principles, and Rules, in: Bodansky, Brunnée and Hey (note 34), 425, at 437.

56 Beyerlin and Marauhn (note 26), at 33-35 and 37-38.

3.1 The Obligation Not to Cause Significant Harm

In 1941 the arbitral tribunal in the *Trail Smelter* case ruled that '[u]nder the principles of international law [...] no state has the right to use or permit the use of territory in such a manner as to cause injury by fumes in or to the territory of another of the properties or persons therein, when the case is of serious consequences and the injury is established by clear and convincing evidence'.[57] Principle 21 of the 1972 *Stockholm Declaration* mirrors this ruling by stating that 'States have [...] the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other states or of areas beyond the limits of national jurisdiction'.[58] This was reaffirmed by Principle 2 of the 1992 *Rio Declaration*.[59] Numerous multilateral environmental agreements have taken up the obligation not to cause harm,[60] and the ICJ has more than once referred to it.[61] The doctrinal underpinning of this key concept is debated, but can be traced back, among others, to a balancing of territorial integrity with territorial sovereignty, perhaps even being interpreted as 'a compromise clearly favouring territorial integrity over territorial sovereignty'.[62]

The obligation prohibits States from causing significant transboundary environmental harm, and at the same time includes a preventive function whereby States have 'to take adequate measures to control and regulate in advance sources of potential significant transboundary harm'.[63] As far as the substantive content of the key concept is concerned, it can be argued that this does not only form part of customary international environmental law,[64] but it also can be considered to be a rule according to Dworkin's theory.[65] As far as the substantive obligation is concerned, there are several aspects which have to be borne in mind. First, the obligation only applies to cases of serious consequence, excluding *de*

---

57 *The Trail Smelter Arbitration Case (Decision of 11 March 1941) (United States v Canada)* (1941) 3 RIAA 1938.

58 See the *Report of the UN Conference on the Human Environment*, Stockholm UN Doc A/CONF48/14/Rev1, at 3.

59 *Report of the United Nations Conference on Environment and Development* (3–14 June 1992) UN Doc A/CONF.151/26/Rev.1 (Vol. I), at 3.

60 By way of example, Article 194(2) of the *United Nations Convention on the Law of the Sea* (UNTS 1833, 397) stipulates: 'States shall take all measures necessary to ensure that activities under their jurisdiction or control are so conducted as not to cause damage by pollution to other States and their environment, and that pollution arising from incidents or activities under their jurisdiction or control does not spread beyond the areas where they exercise sovereign rights in accordance with this Convention'. Article 3 of the *Convention on Biological Diversity* (UNTS 1760, 79) reads: 'States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction'.

61 ICJ, *Legality of the Threat or Use of Nuclear Weapons [Advisory Opinion]* [1996] ICJ Rep 226, at 241 *et seq* (para. 29); *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v Slovakia) (Judgment)* [1997] ICJ Rep 7, at 41 (para. 53).

62 Marauhn and Beyerlin (note 26), at 40.

63 G. Handl, 'Transboundary Impacts', in: Bodansky, Brunnée and Hey (note 34), 531, at 539.

64 Marauhn and Beyerlin (note 26), at 44; Bodansky (note 8), at

65 See above notes 51 and 53.

minimis injury, and requiring significant harm,[66] which is, however, difficult to define.[67] Second, the obligation entails a disregard of the requirement of due diligence;[68] i.e. 'the injury incurred must have been foreseeable for the state of origin [... in light of] today's best scientific knowledge'.[69] Third, while the arbitral tribunal in the *Trail Smelter* case required 'clear and convincing evidence',[70] some argue that the burden of proof should be commensurate with the seriousness of the impending harm; that the higher the probability of the occurrence of the respective harm, the lower the required standard of proof should be,[71] a position which is not yet par for customary international law.[72]

Apart from the substantive obligations, doctrine and political practice have derived a number of procedural obligations from the overall concept. These include the obligations to consult, to exchange information, to notify of an emergency and to give early warnings, to perform a transboundary environmental impact assessment, and to ensure transboundary rights of participation as well as access to justice.[73] While the obligations to consult and to exchange information may today be considered to be part of customary international law,[74] access to justice in a transboundary international context is so far-reaching that it can only be treaty-based.[75] In the *Case concerning Pulp Mills on the River Uruguay* the ICJ confirmed that the obligation to perform a transboundary environmental impact assessment is rooted in customary international law.[76]

The substantive obligation not to cause significant harm to cyberspace can be plausibly applied, subject to a number of conditions, which are inherent prerequisites of the obligation. Among them is the jurisdictional aspect of activities originating in one State and having an effect in another, or at least in an area beyond the national jurisdiction of the originating State. Linked to this prerequisite is the issue of attribution. While

66 Marauhn and Beyerlin (note 26), at 41.

67 Handl (note 64), at 535-538.

68 T. Koivoruva, 'Due Diligence', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2010) (accessed on 30/10/2013). Koivoruva explains that a breach of due diligence obligations 'consists not of failing to achieve the desired result but failing to take the necessary, diligent steps towards that end' (*Ibid*., at para. 3).

69 Beyerlin and Marauhn (note 26), at 43.

70 *The Trail Smelter Arbitration Case (Decision of 11 March 1941) (United States v Canada)* (1941) 3 RIAA 1938, at 1965.

71 For a discussion see P.W. Birnie, A.E. Boyle and C. Redgwell, *International Law and the Environment* (3rd ed, Oxford 2009), at 152 *et seq*.

72 Beyerlin and Marauhn (note 26), at 43-44.

73 Handl (note 64), at 540-544; Beyerlin and Marauhn (note 26), at 44-45.

74 Beyerlin and Marauhn (note 26), at 45.

75 For a comprehensive discussion see Beyerlin and Marauhn, *Ibid*., at 234-239.

76 *Case concerning Pulp Mills on the River Uruguay* (*Argentina v Uruguay*) (Judgment of 20 April 2010), at paras. 162-164, available at <http://www.icj-cij.org/docket/files/135/15877.pdf> (accessed on 30/10/2013); for a discussion of the case see P.M. Vernet, 'Pulp Mills on the River Uruguay (*Argentina v Uruguay*)', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2010) (accessed on 30/10/2013).

these two aspects alone may raise concerns about application of the obligation not to cause significant harm, the preventive and procedural obligations deriving therefrom, in particular to the extent that they are qualified by reference to the threshold of due diligence are *prima facie* more suitable for application to cyberspace.

3.2 The Precautionary Approach

Principle 15 of the *Rio Declaration* reads as follows: 'In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation'.[77] Framed in treaty law, Article 3(3) of the 1992 UN *Framework Convention on Climate Change*[78] states that the 'Parties should take precautionary measures to anticipate, prevent or minimize the causes of climate change and mitigate its adverse effects. Where there are threats of serious or irreversible damage, lack of full scientific certainty should not be used as a reason for postponing such measures'. Similarly, Articles 10(6) and 11(8) of the 2000 *Cartagena Biosafety Protocol*[79] to the *Convention on Biological Diversity* expressly take up the precautionary approach stating that '[l]ack of scientific certainty due to insufficient relevant scientific information and knowledge regarding the extent of the potential adverse effects of a living modified organism on the conservation and sustainable use of biological diversity [...] shall not prevent that Party from taking a decision [...] in order to avoid or minimize such potential adverse effects'. Case law has essentially taken the same approach to precautionary action as treaty law. Thus, the *Southern Bluefin Tuna* case the International Tribunal for the Law of the Sea stated in 1999 that, notwithstanding 'scientific uncertainty regarding measures to be taken to conserve the stock of southern Bluefin tuna and [...] although the tribunal cannot conclusively assess the scientific evidence presented by the parties, it finds that measures should be taken as a matter of urgency to preserve the rights of the parties and to avert further deterioration'.[80]

---

77 *Report of the United Nations Conference on Environment and Development* (3–14 June 1992) UN Doc A/CONF.151/26/Rev.1 (Vol. I), at 6.

78 UNTS 1771, 107.

79 UNTS 2226, 208.

80 *Southern Bluefin Tuna Cases (New Zealand v Japan*; *Australia v Japan*) (Provisional Measures) ITLOS Cases Nos 3, 4 (27 August 1999), at paras. 79 *et seq*. In earlier cases, the ICJ did not yet fully take up the precautionary approach, such as in the *Request for an Examination of the Situation in Accordance with Paragraph 63 of the Court's Judgment of 20 December 1974 in the Nuclear Tests (New Zealand v France*) Case (Order) [1995] ICJ Rep 288, where Judges Weeramantry (*Ibid*., at 342 *et seq*) and Palmer (*Ibid*., at 412) referred to the precautionary approach in their dissenting opinions, and in the *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v Slovakia*) (Judgment) [1997] ICJ Rep 7, where only the parties (Hungary and Slovakia) invoked the precautionary principle, but the Court did not deal with it in detail.

The precautionary approach aims to ensure that States do not only ward off identified environmental dangers, but also take early action to prevent the emergence of such dangers. In other words, the precautionary approach responds to the 'limitations of science in assessing global ecological risks'.[81] It goes beyond the obligation to prevent significant harm, which applies in situations where the scientific basis as such is clear and it only remains uncertain whether an identified environmental harm will indeed materialise.[82]

The consequences arising from the precautionary approach have been read differently. While some understand it only to mean that uncertainty is no excuse for inaction,[83] others interpret it as a concept that 'uncertainty justifies action',[84] and some even read it as a 'duty [...] to take action'.[85] At least the latter interpretation of the precautionary approach is difficult to prove as being already part of customary international law.[86] As has been illustrated, numerous substantive and procedural sub-sets of obligations can be derived from the precautionary approach, such as the obligation to grant equal access to environmental information, the application of a transboundary environmental impact assessment, and the requirement to apply the best available technology.[87] While it has been argued that the precautionary approach may even shift the burden of proof to the entity performing the potentially risky activity, the ICJ in its *Pulp Mills on the River Uruguay* judgment of 20 April 2010,[88] although in principle accepting that 'a precautionary approach may be relevant'[89] clearly stated that 'it does not follow that it operates as a reversal of the burden of proof'.[90]

The precautionary approach is ultimately appropriate for regulating cyberspace. Its potential to address scientific or technological uncertainty is highly relevant to managing cyber-based activities. It must, however, be borne in mind that the uncertainty in the context of cyberspace most often relates to the question of attribution, and less to a lack of knowledge in respect of the actual operation of cyberspace. The precautionary approach can in principle be considered to be part of customary international environmental law, but the uncertainties surrounding its normative quality, status and effects nevertheless

81 Beyerlin and Marauhn (note 26), at 52.

82 *Ibid*., at 53.

83 J.B. Wiener, Precaution, in: Bodansky, Brunnée and Hey (note 34), 597, at 604 *et seq*.

84 D. Bodansky, 'Deconstructing the Precautionary Principle', in: D.D. Caron and H.N. Schreiber (eds.), *Bringing New Law to Ocean Waters* (Law of the Sea Institute, University of California 2004), 381, at 385.

85 Illustrated by Beyerlin and Marauhn (note 26), at 54, referring to A. Trouwborst, *Precautionary Rights and Duties of States* (Brill 2006), at 159 *et seq* and 287.

86 Beyerlin and Marauhn (note 26), at 56 argue that the concept as such 'is an emerging rule of customary international environmental that can claim eminent importance'.

87 *Ibid*., at 54.

88 *Case concerning Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment of 20 April 2010), available at <http://www.icj-cij.org/docket/files/135/15877.pdf> (accessed on 30/10/2013).

89 *Ibid*., at para. 164.

90 *Ibid*.

make its applicability in cyberspace questionable. It is much more reasonable to consider the ideas underlying the precautionary approach as guiding principles for the envisaged regulation of cyberspace.

3.3 Ensuring Accountability of Private Actors: The Polluter Must Pay

In contrast to the already discussed concepts of 'no harm' and 'precautionary action', the concept that the polluter must pay does not address inter-governmental relations but imposes an obligation upon States to ensure that, in municipal law, other entities do not escape their responsibility. As framed in Principle 16 of the 1992 *Rio Declaration*, '[n]ational authorities should endeavour to promote the internalisation of environmental costs and the use of economic instruments, taking into account the approach that the polluter should, in principle, bear the costs of pollution'.[91] In treaty law, the 1990 *International Convention on Oil Pollution Preparedness, Response and Cooperation*[92] in its preamble requires those States party to it to take account of 'the 'polluter pays' principle as a general principle of international environmental law'.[93] Also, as can be taken from Article 2(2)(b) of the 1992 *Convention for the Protection of the Marine Environment of the North-East Atlantic*,[94] the parties to this multilateral agreement 'shall apply [...] the polluter pays principle, by virtue of which the costs of pollution prevention, control and reduction measures are to be borne by the polluter'.

As to the normative status of the obligation to ensure that the polluter is held responsible, this can easily be read as a rule as outlined above.[95] Most authors, not least in light of the wording in Principle 16 of the *Rio Declaration*, doubt that the obligation has already obtained the status of customary international law.[96] Relying on the reference to the obligation in the *International Convention on Oil Pollution Preparedness, Response and Cooperation*, it is debateable whether the obligation is a general principle of law according to Article 38(1)(c) of the ICJ Statute.[97] Bodansky, being sceptical of the customary international law status of some of the key concepts discussed here, raises the question of how to consider norms which 'do not reflect behavioural regularities, and therefore do not qualify as customary norms'.[98] He describes them as 'attitudinal regularities among states and other international actors',[99] but still considers them to

91 *Report of the United Nations Conference on Environment and Development* (3–14 June 1992) UN Doc A/CONF.151/26/Rev.1 (Vol. I), at 6.

92 UNTS 1891, 51.

93 Preamble, indent 7.

94 UNTS 2354, 67.

95 See Beyerlin and Marauhn (note 26), at 59.

96 *Ibid*., at 59.

97 UNTS 33, 993.

98 Bodansky (note 8), at 199-200.

99 *Ibid*., at 200.

have an effect upon the behaviour of States.[100] From a doctrinal perspective, it seems to be more convincing to consider them as general principles, understood as norms common to the major legal systems across the globe, thus emerging from municipal law, but capable of being transposed to the international level.[101] This is even more convincing, since the obligation that the polluter must pay is directed to be implemented at the national level; thus, it is the typical kind of norm-manoeuvring between municipal and international levels.

In terms of its substance, the obligation discussed here is designed to impact the behaviour of private actors, 'allocating the costs of preventive or remedial environmental measures to the polluter'.[102] This 'implies a significant negative economic incentive'[103] for private actors to abstain from pollution. Since environmental degradation and related pollution typically result from the behaviour of private actors, the obligation to impose the financial burden for any such pollution on those actors seems to be more than obvious in order for States to have meaningful instruments at hand to comply with their international obligations. The concept 'polluter pays' is thus instrumental rather than substantive as far as relations between States are concerned.

Bearing in mind that cyberspace activities are likewise largely performed by private actors, the obligation to hold them responsible for any damage they cause to cyberspace in the same way the 'polluter pays' concept provides for damage caused to the environment is appealing. Whether the concept is directly applicable to cyberspace is as questionable as with regard to the other concepts discussed above.

3.4 Sustainable Development

The concept of sustainable development has become a buzzword of international environmental law. It is perhaps the most widely spread term in this field of law, and at the same time a truly diffuse one. In international environmental law it is generally used to reflect the interdependence between the protection of the environment and economic development. In the words of the *Rio Declaration*, '[i]n order to achieve sustainable development, environmental protection shall constitute an integral part of the development process and cannot be considered in isolation from it'.[104] More generally, sustainable development today 'is broadly understood as a concept that is characterized

100 *Ibid*., at 202.

101 For a discussion of the notion of general principles see G. Gaja, 'General Principles of Law', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2007), in particular at para. 16 (accessed on 30/10/2013); see also A. Pellet, 'Article 38', in: A. Zimmermann/C. Tomuschat/K. Oellers-Frahm (eds.), *The Statute of the International Court of Justice* (Oxford 2006), at paras. 250-264, addressing the transposability to international law at paras. 262-264.

102 Beyerlin and Marauhn (note 26), at 58.

103 *Ibid*., at 58.

104 Principle 4, *Report of the United Nations Conference on Environment and Development* (3–14 June 1992) UN Doc A/CONF.151/26/Rev.1 (Vol. I), at 4.

by (1) the close linkage between the policy goals of economic and social development and environmental protection; (2) the qualification of environmental protection as an integral part of any developmental measure, and vice versa; and (3) the long-term perspective of both policy goals, that is the States' inter-generational responsibility'.[105]

The normative quality and status of the concept of sustainable development is highly controversial. There seems, however, to be a tendency not to overstretch the normativity of sustainable development. In Dworkin's construct it would not be attributed the status of a rule, but rather of a principle, and whether it really has become part of customary international law is debatable. The ICJ did not rule on its status in the *Case concerning the Gabčíkovo-Nagymaros Project*,[106] and whether the Court shares the view[107] that sustainable development is 'a part of modern international law by reason not only of its inescapable logical necessity, but also by reason of its wide and general acceptance by the global community'[108] (as phrased by Judge Weeramantry in his separate opinion) is doubtful.

Even if the concept of sustainable development provides a guideline for making, interpreting and perhaps even applying international law, and does not establish a rule which has a direct impact on State behaviour, it opens up a useful perspective which may also be taken into account when regulating cyberspace. Both the environment and cyberspace are a limited resource available for economic activities of human beings; at the same time their preservation and availability necessitate positive measures by States, including investment in order to make them sustainable. It is against this background that the notion of sustainable use can be applied,[109] which aims to ensure that resources are not exploited beyond their capacities, referring to sustained and optimal exploitation rather than unlimited exploitation.

3.5 The Common Heritage Approach

It has been debated whether cyberspace should be perceived as part of the global commons.[110] The global (or international) commons are areas open to use by all

105 U. Beyerlin, 'Sustainable Development', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2009), at para. 9 (accessed on 30/10/2013).

106 *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v Slovakia*) (Judgment) [1997] ICJ Rep 7, at 78 (para. 140).

107 This is the position of P. Sands, *Principles of International Environmental Law* (2nd ed, Cambridge 2003), at 254.

108 *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v Slovakia*) (Judgment) [1997] ICJ Rep 7, at 95.

109 Beyerlin and Marauhn (note 26), at 82.

110 For a discussion see, among others, M. Mueller, J. Mathiason and H. Klein, The Internet and Global Governance: Principles and Norms for a New Regime, (2007) Global Governance 13, 237.

States. They include the high seas, Antarctica, and outer space.[111] In international law the commons are normally considered through the lens of the common heritage approach.[112] The approach is not fully defined under international law,[113] but a number of characteristics can be identified which are relevant for commons, subject to the common heritage approach: First, these areas are not subject to the exercise of sovereignty or sovereign rights; second, States are subject to a duty of international cooperation with regard to the use of such commons, which are often internationally managed and subject to regulated use, the effect of which often is to distribute the benefits from such use; third, use should normally be peaceful only; fourth, use of the commons should preserve them and their benefits for future generations.[114] While these are common characteristics of the common heritage approach,[115] they are not necessarily part of customary international law; indeed, they are primarily treaty-based and it is difficult to prove that in parallel they also exist as part of customary international law.

Whether or not the common heritage approach can be applied to cyberspace is also doubtful. As has been pointed out, 'attempts have been made to invoke this principle with respect to technology, cultural property, and the protection of the environment', but 'the main impact of the common heritage principle remains the establishment of an international administration for areas open to the use of all States'.[116] While 'international law continues to struggle with "collective" or "community" aspirations',[117] the concept has to some extent at least found its way into treaty law, and 'the emerging normative patterns may eventually feed back into the development of customary law'.[118]

4. Applying Existing Law or Making Future Law?

Having outlined the substance of five key concepts of international environmental law, the question remains as to what can be drawn from this for the regulation of peaceful use of cyberspace. Largely, this is not about the application of international environmental law to cyberspace. No question arises in this regard if cyber-activities have a negative impact on the environment; customary and treaty-based international environmental law will be applicable. If, however, no such negative impacts materialise

111 See J. Brunnée, 'Common Areas, Common Heritage, and Common Concern', in: Bodansky, Brunnée and Hey (note 34), 550, at 557-561.

112 See generally R. Wolfrum, 'Common Heritage of Mankind', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2009) (accessed on 30/10/2013).

113 *Ibid.*, at para. 11.

114 *Ibid.*, at paras. 14-24.

115 Brunnée (note 113), at 561-564.

116 Wolfrum (note 114), at para. 1.

117 Brunnée (note 113), at 572.

118 *Ibid.*, at 572.

or are expected, reference to international environmental law is only about the parallels between this area of the law and the regulation of cyberspace.

In light of the parallels between the natural environment and cyberspace outlined in the introductory part of this chapter, discussing the transposability of customary international environmental law to the emerging rules on cyberspace is a meaningful effort in the process of making pertinent future law. In this short section, three relevant problem areas will be taken up and discussed: First, to the extent that international environmental law is a specialised field of public international law, the question arises whether *lex specialis* can serve as a model for prospective law-making. Second, the transferability or transposability of rules developed in one area of the law to another depend on parallels between the two areas; not just the parallels between the natural environment and cyberspace, but parallels in respect of the relevant regulatory approaches. Third, differences between the subject matters under consideration and pertinent regulatory approaches must be taken into account in order to 'mind the gap' between a seemingly plausible idea and its realisation.

4.1 International Environmental Law as a Specialised Part of Public International Law (*lex specialis*)

International environmental law is part of public international law. As a matter of course this first means that general public international law remains applicable unless there are more specific rules developed for the protection of the environment which prevail on the basis of the rule *lex specialis derogat legi generali*.[119] This rule does not only apply between various treaties, but also whenever conflicts arise between treaty law and customary international law. The application of this rule, however, also depends on whether or not international environmental law is indeed a distinct field.

In their opening chapter of the *Oxford Handbook of International Environmental Law*, its editors refer to 'new types of concerns, new actors, and new standard-setting and compliance processes'[120] as well as to the 'very terminology of international environmental law'[121] to demonstrate the distinctiveness of this area of the law. The editors of the Handbook point out that, in order to address international environmental problems, 'we need complex regulatory regimes, which involve more flexible and dynamic standard-setting processes, and we need to take a pragmatic and forward-looking approach'.[122] In essence, international environmental law does not only include

119 See N. Matz-Lück, 'Treaties, Conflicts between', in: R. Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, online edition, available at <http://opil.ouplaw.com/home/epil> (Oxford 2010) (accessed on 30/10/2013), at para. 16.

120 D. Bodansky, J. Brunnée and E. Hey, 'International Environmental Law – Mapping the Field', in: Bodansky, Brunnée and Hey (note 34), 1, at 24.

121 *Ibid*., at 24.

122 *Ibid*., at 24.

a number of substantive and procedural features which make it a distinct area of public international law, but they also bring about the need for an institutional setting that is, at least in part, tailor-made.

The question can also be asked whether these particular characteristics of international environmental law are unique or whether this body of law can serve as a model for other emerging fields of international law. While international environmental law has 'adapted to significant societal changes, which are associated with the processes of globalization',[123] it is not a solitary part of international law. Indeed, there is potential for 'cross-fertilization'[124] between international environmental law and other fields of international law.

It is precisely the characteristics of international environmental law just described, which explain and underline how it is difficult to directly apply customary rules of international environmental law to cyberspace: international environmental law addresses problems which are unique and which therefore have generated a set of rules which differs from general international law. It has addressed technological and societal change in an unprecedented way and thus, as a matter of principle, seems to be suited to being transferred to the regulation of cyberspace.

4.2 The Transferability of Customary Rules of International Environmental Law

Whether or not and to what extent customary rules of international environmental law can be transferred to the regulation of peaceful uses of cyberspace necessitates a comparative analysis, focusing on the parallels and differences not only between the subject-matters at issue but also in respect of the regulatory approach; it is much about distinguishing, and in the case of parallels identified, it is about adapting rules rather than about their transfer or transposition.

In the introductory part of this chapter a number of parallels between the natural environment and cyberspace were identified. This part of the chapter focuses on potential regulatory parallels.

The first parallel concerns the tension between legal certainty and adaptability: international environmental law, if it is meant to be legally binding, must provide legal certainty for States to create their own national regulatory environment which enables business and industry to operate while at the same time protecting the environment.[125] There is also technological and societal change, which requires adaptation to changing

123 *Ibid.*, at 25.

124 *Ibid.*, at 25.

125 On the quest for legal certainty as one of the rationales for negotiating agreements in international environmental law, see Bodansky (note 8), at p. 154.

circumstances. International environmental law is capable of addressing this tension by combining customary international law and treaty-based law, and by applying rather flexible law-making strategies also at the treaty-level, such as the 'framework convention and protocol approach' or the 'convention and annexes approach'.[126] This two-fold approach to law-making is also suitable for cyberspace, which is a rapidly changing field of technology, nevertheless requiring legal certainty for its economic use.

A second parallel concerns the use of the respective environment by private actors. Indeed, a lot of environmental problems 'result primarily from private, rather than governmental, conduct'.[127] The same applies to peacetime activities in cyberspace. Thus, the concept of 'polluter pays' is essential since it not only enables States to address private actors and efficiently allocate the costs of activities making use of a common resource,[128] but also ensures that the link between international, governmental and private activities is addressed.

The obligation not to cause significant harm can be read along the same lines. The 'no harm' concept includes a preventive element[129] which is ultimately important in a multi-layered environment impacted upon by technology. It imposes upon States an obligation to regulate the use of such natural or technological space with due diligence[130] to avoid damage arising in other States. While due diligence does not require States to fully address technological or scientific attribution, it requires them to at least develop a regulatory approach. This can be based on fictitious (normative) attribution rather than factual attribution alone.

A fourth parallel can be identified with regard to the precautionary approach. Scientific uncertainty exists in numerous fields, and the regulatory approach must be to overcome such scientific uncertainty by normative criteria, at least in situations which include the risk of enormous damage. In international environmental law, the precautionary approach has successfully been developed and applied. It has, however, so far not impacted upon many other areas of the law. Technology-related regulation is, as a matter of principle, open to precautionary considerations which allow for flexibility in the development and application of new technology, while at the same time not preventing governments from regulating such technologies simply in light of scientific or technological uncertainties.[131]

126 Beyerlin and Marauhn (note 26), at 270-273.

127 Bodansky, Brunnée and Hey (note 121), at 24.

128 See D. Shelton, Equity, in: Bodansky, Brunnée and Hey (note 34), 639, at 656.

129 Handl (note 64), at 538-540.

130 Koivoruva (note 69), passim.

131 Wiener (note 84), at 599-601.

4.3 Mind the Gap! The Issue of Territoriality

Having identified parallels, there must be reference to differences which have to be taken into account. Cyberspace is not a natural environment, it is man-made; furthermore, the natural environment is already in place, whereas cyberspace is still being developed, and it is costly. These are factual differences with limited impact on regulatory strategies.[132]

Much more important is the issue of territoriality. Most of international environmental law has been developed in the context of neighbouring States, and with respect to transboundary effects on the environment. The regulation of transboundary activities is based on pre-existing territoriality. Even though it is sometimes difficult to trace the causes of environmental degradation, as may be obvious in the context of transboundary air pollution, there is at least a territorial link that can be made use of. This has been demonstrated when addressing the acid rain phenomenon both in Europe and in North America.[133] The regulation of global environmental problems has, however, been less successful, as can be seen in the current failure to establish a meaningful regime addressing climate change.[134] In this context there is very little territoriality on which regulation can be based, quite in contrast to the management of biodiversity where States have agreed to rely upon territorial sovereignty over biological resources rather than applying the principle of common heritage.[135] This may be taken as proof of the hypothesis that the regulation of the international environment has always been more successful when there was a link with territoriality; in the absence of such a link, regulation has failed more often than is desirable.

Drawing conclusions for the regulation of cyberspace does not mean simply pointing to the absence of territoriality in cyberspace, but it illustrates the need not to ignore territory when developing a peacetime regime for cyberspace. Cyberspace is not fully detached from territory; in particular, hardware has a location. Thus, the question arises as to whether and to what extent territory can be made use of in the regulation of cyberspace. When drawing parallels from international environmental law to cyberspace, lawmakers should mind the gap in respect of territoriality.

5. Conclusions

This chapter has raised the question of to what extent international environmental law can contribute to the regulation of peaceful uses of cyberspace. While there are indeed parallels between these areas of the law with respect to the subject matter concerned

132 See above, introduction.

133 Beyerlin and Marauhn (note 26), at 149-154.

134 *Ibid*., at 159-171.

135 T. Marauhn, ‚Die Erhaltung der biologischen Vielfalt und die nachhaltige Nutzung ihrer Bestandteile. Rechtsinstitute der Nachhaltigkeit auf der Grundlage des UN-Übereinkommens über die biologische Vielfalt‘, in: Klaus Lange (ed.), *Nachhaltigkeit im Recht: eine Annäherung* (Nomos 2003), at 87-108.

and existing or future regulatory approaches, it is difficult to apply international environmental law directly to cyberspace. Rather, some of the key concepts, some of them customary international law, can be made use of and taken as a model for the development of a peacetime cyberspace regime.

Among these key concepts, the obligation not to cause significant transboundary harm, the precautionary approach, and the obligation to ensure that the polluter is held accountable ('polluter pays') are the most promising, but some guidance can also be derived from the concept of sustainable development and the concept of common heritage of mankind.

Having identified parallels and differences, the responsibility for a future cyberspace regime is put into the hands of law-makers, who can build on existing parallels, not only in substance but also with regard to the various legal sources at hand. It has been shown that international environmental law has successfully built on a combination of customary and treaty-based law as well as on a combination of general concepts and tailor-made regimes. This appears to be a promising approach also for the regulation of cyberspace.

There is one major stumbling block, which has been identified by this chapter: the issue of territoriality. Successful environmental regulation and successful application of customary international environmental law have always benefited from a territorial link. Global environmental problems without any territorial link have been hard to establish, and when established have not in themselves been successful, as has been shown with regard to the climate change regime.

In sum, international environmental law can be made use of as a source of creativity for the development of regulatory approaches to cyberspace, but it has limited direct relevance as of today.

Jan Klabbers

Responsibility of States and International Organisations in the Context of Cyber Activities with Special Reference to NATO

1. Introduction

The aim of this chapter is to explore issues of responsibility in cyber operations in connection with what used to be called the Atlantic Alliance, in particular the distribution of responsibility between North Atlantic Treaty Organization (NATO) and its Member States. The setting is hypothetical, and the possible scenarios discussed will be hypothetical as well. I will focus on cyber attacks, self-defence and United Nations (UN) Security Council-authorised military operations in order to explore issues of responsibility, but it is important to realise that other issues may also present themselves, such as the use of hacking for intelligence purposes and the use of cyber techniques in anti-terrorism campaigns.

While there may be a need to develop new or adapt existing rules of substantive international law (primary rules, in Hart's terminology[1]) to the exigencies of cyber operations, be it in terms of *jus ad bellum* or *jus in bello*, I will work on the presumption that this does not apply to the secondary rules of international law – and the rules on responsibility, be they of States or international organisations, typically fall into this latter category. These are like the rules of the road, applicable to all vehicles without prejudice to the possibility of specific rules applying to specific vehicles.

The main focus will rest on the division of responsibility between NATO and its Member States, and much of this will depend on the precise relationship between them, as arranged for in the various international agreements. Here then cyber operations may force a re-consideration of existing practice: it is not impossible that NATO and its Member States might wish to put something on paper regarding the division of labour between them should a cyber attack triggering the right to self-defence occur or, which is not *a priori* excluded either, should NATO and its Member States decide to engage in cyber operations themselves, e.g. during the course of a UN Security Council-authorised military operation. A division of labour may come with claims of limited liability,[2] or it may specify that action by one is to be regarded as action by another. Or

1 See H.L.A. Hart, *The Concept of Law* (Oxford: Clarendon Press, 1961).

2 With the financial institutions, a limited liability clause is often already provided for in the constituent instrument. See, e.g., Article 3(3) of the *Agreement establishing the International Fund for Agricultural Development*: 'No Member shall be liable, by reason of its membership, for acts or obligations of the Fund.' A useful discussion of the rationales behind such a clause is contained in C.F. Amerasinghe, *Principles of the Institutional Law of International Organizations*, 2d ed. (Cambridge University Press, 2005), chapter 9.

such arrangements may remain silent on issues of responsibility, leaving it to courts (if any) to figure out what to do *ex post facto*, in much the same way as the Dutch Supreme Court recently had to decide on the division of responsibility between the UN and the Netherlands in three cases involving the Srebrenica massacre.[3]

Hence, the main thrust of this chapter will be to address the law of international responsibility, both as it relates to States and as it relates to international organisations such as NATO. Before going into some detail about these two regimes, some introductory conceptual remarks are in order. Thereafter, the legal principles identified as possibly relevant will be discussed and, as a heuristic device, I will briefly discuss military cyber operations in various possible configurations.

2. Conceptual Issues

While the origins of modern international law are often said to go back to the seventeenth century and in particular to the Peace of Westphalia, which inaugurated a system of sovereign States, much of the flesh on these bare bones of the system was developed by international tribunals, and for the better part these only emerged during and after the nineteenth century.[4] Such tribunals were particularly instrumental in developing the so-called secondary rules of international law: rules relating to the making, application and enforcement of international law, including the rules on responsibility.

During this period, States were considered the only relevant actors in international law, so it is no surprise that the system of State responsibility developed during these years. Over time, and through the activities of many courts and tribunals, the law on State responsibility crystallised into two foundational ideas.[5] First, States can only be held responsible for internationally wrongful acts, i.e. for violations of international legal obligations incumbent on them. Nothing more is required, and nothing less will do. Thus, nasty acts, immoral acts, or acts causing serious damage will not result in State responsibility, unless these acts also go against an international legal obligation of the State. But wrongfulness itself is sufficient: it need not result in damage in order to trigger the responsibility of the State.

Second, the wrongful act must be attributable to the State. In other words: the State cannot be held responsible for the acts of its citizens if they are acting in a private capacity. As a matter of course, all acts of State organs and State officials will be attributed to the State, and this includes even the acts of State organs that are constitutionally

3 See e.g. *State of the Netherlands* v *Hasan Nuhanovic*, Netherlands Supreme Court, judgment of 6 September 2013, available in English at http://www.rechtspraak.nl/Organisatie/Hoge-Raad/OverDeHogeRaad/publicaties/Documents/12%2003324.pdf (last visited 2 October 2013).

4 See generally Jan Klabbers, *International Law* (Cambridge University Press, 2013).

5 See generally James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press, 2002).

independent, such as courts. A recent relevant decision of the International Court of Justice (ICJ) underlined as much when it suggested that the Italian Court of Cassation had wrongly refused to uphold the sovereign immunity of Germany for acts committed during the Second World War.[6]

If State responsibility has a long and highly respectable pedigree, the responsibility of international organisations, by contrast, was only recently discovered as an area of interest. Early efforts to map and chart the responsibility of international organisations invariably lapsed quickly into discussions of the responsibility of Member States for acts of the organisation.[7] It required the general recognition that international organisations could also be seen as independent relevant actors ('subjects' of international law, in jargon) and, more specifically, the realisation that international organisations could actually engage in conduct that would merit the applicability of a responsibility regime, before the responsibility of international organisations came to be considered as a serious topic in international law. In other words, international law started to think seriously about organisational responsibility when it became clear that organisations could do wrong, and by general acclamation this insight started to dawn on international lawyers at the earliest in the mid-1980s.[8]

During international law's formative years (i.e. the late nineteenth and early twentieth centuries), relations between States were often modelled on private or civil law paradigms. International law was, as one luminary suggested,[9] essentially private law between public actors, and it is fair to say that much of international law still carries traces (and sometimes considerably more than traces) of this classic conception. This applies to the law of treaties, which is modelled on domestic contract law, and it applies to the law of State responsibility as well. This is largely – and roughly – modelled on tort law, if only because a criminal law paradigm would be inappropriate in relations between sovereign States, and because a public law paradigm had hardly been discovered at the time.[10]

After the Second World War, the International Law Commission (ILC), a new UN body consisting of respected and elected international lawyers, was given the task of codifying and developing international law, much of which had remained customary and unwritten. Among the topics identified for such a project of codification, laced perhaps with some progressive development, was the law on State responsibility. It took a while,

6 See *Jurisdictional Immunities of the State* (Germany v Italy; Greece Intervening), judgment of 3 February 2012.

7 See e.g. Clyde Eagleton, 'International Organization and the Law of Responsibility', (1959/I) 76 *Recueil des Cours*, 319-425; Konrad Ginther, *Die völkerrechtliche Verantwortlichkeit internationaler Organisationen gegenüber Drittstaaten* (Vienna: Springer, 1969).

8 See e.g. Jan Klabbers, *An Introduction to International Institutional Law*, 2d ed. (Cambridge University Press, 2009), 271-293.

9 See T.E. Holland, *The Elements of Jurisprudence*, 13th ed. (Oxford: Clarendon Press, 1924).

10 The distinction between these three paradigms is elucidated in Peter Cane, *Responsibility in Law and Morality* (Oxford: Hart, 2002).

but by 2001 the ILC presented a complete set of articles on State responsibility to the world. These are generally taken to reflect pre-existing and simultaneously developing customary international law on the topic, and while the ILC strategically decided not to call for the convocation of a conference to conclude a convention on State responsibility, the articles are considered highly authoritative.[11]

A year earlier, the ILC decided to place the topic of the responsibility of international organisations on its agenda, and appointed Professor Giorgio Gaja (now a judge at the ICJ) as its Special Rapporteur. Gaja produced a number of reports, and by 2011 the ILC adopted a complete set of draft articles. As with the responsibility of States, there seems little reason to presume that the articles will be given the form of a legally binding convention; unlike the articles on State responsibility, however, Gaja's work is not deemed highly reflective of customary international law. The main gripes are twofold. First, since there was not much practice to begin with, the articles on responsibility of international organisations are considered very much the brainchild of Gaja and his team. They lack, in other words, the authority that stems from long and consistent usage. Second, many organisations feel that the articles represent a straitjacket; useful generally perhaps, but not for their specific issues. In other words, the articles represent a one-size-fits-all approach but international organisations claim – and not without justification – that they are too widely divergent in nature, composition and tasks to make this one-size-fits-all approach workable.[12]

In a sense, Gaja's project never stood a chance: it had to accommodate too many unresolved tensions in the law. For instance, given that there was already a set of articles on State responsibility outlining how responsibility would be incurred, what its consequences are, *et cetera*, it stood to reason to expect the articles on the responsibility of organisations not to depart too much from those basic principles. It would be awkward, for instance, to have State responsibility based on an internationally wrongful act, but to base the responsibility of organisations on something else: negligence, criminal intent, or even strict liability.[13] And indeed, this is the approach followed by Gaja: the basic set-up of the system follows the articles on State responsibility.

But closely following the articles on State responsibility creates problems of its own. For one thing, international organisations are not States; instead, they are created by States, and while States continue to exercise some influence on the activities of organisations,

---

11 The work was finalised under the stewardship of Special Rapporteur James Crawford. See Crawford, Articles on State Responsibility.

12 These critiques invariably transpire in discussions with legal advisers of international organisations. See also Niels M. Blokker, 'Preparing Articles on Responsibility of International Organizations: Does the International Law Commission take International Organizations Seriously? A Mid-term Review', in Jan Klabbers and Åsa Wallendahl (eds.), *Research Handbook on the Law of International Organizations* (Cheltenham: Edward Elgar, 2011), 313-341.

13 Strict liability is rare in international law generally: one of the few examples generating strict liability is the sending of satellites into orbit. See Klabbers, International Law, at 127.

nonetheless organisations have their own systems of decision-making and institutional structures.[14] Second, and arguably more seriously, while it makes some sense (at least historically) to regard States, in their dealings *inter se*, as private actors writ large, the civil law paradigm that is reflected in the articles on State responsibility cannot be applied without modification to international organisations. These, after all, perform quintessentially public tasks; they exercise public power, and thus a regime more geared towards controlling public power would have been more appropriate. But that would have meant writing radically different rules for organisations than for States.

This point, important as it is, should perhaps not be exaggerated: States, even in their relations *inter se*, sometimes address exercises of public power (think of human rights treaties, or treaties for the protection of the commons); their relations cannot be modelled on private law analogies alone.[15] But even so, this arguably testifies more to the problem of fit that human rights law and environmental law experience in the global legal order,[16] than that it undermines the proposition that international organisations exercise public power, and thus that a regime outlining the responsibility of international organisations ought to take this into account.

Indeed, already when drafting the articles on State responsibility, the ILC realized that a pure private law paradigm would be unsatisfactory, and introduced something of a public order conception in its conceptualisation.[17] It suggested that primary obligations (the substantive rules of international law) are primarily owed to treaty partners, and therewith typically modelled on private law relations. But above and beyond, it suggested that once a State does something wrong, the international community at large becomes involved: the law on State responsibility gives a voice to States other than the one directly injured, and more generally, the legal relationships created by the law on responsibility are deemed to operate on this 'higher' plane. Concretely, a breach of a treaty provision engages the relations between the treaty partners, but when it comes to assessing the consequences of the breach, the discussion moves to the level of State responsibility, and that level pits the wrongdoing State against the international community at large. The treaty partner has a stake in seeing the provision upheld, but the international community has a stake in seeing the sanctity of the treaty upheld.

14 See Catherine M. Brölmann, *The Institutional Veil in Public International Law: International Organisations and the Law of Treaties* (Oxford: Hart, 2007).

15 The reverse, incidentally, also holds true: to some extent international organisations deal with States and other international organisations in ways which can be likened to classic inter-State intercourse, and for which a private law paradigm of responsibility is thus not inappropriate. The main problem then with the regime on responsibility of international organisations is that it focuses too much on these private law-type relations, and too little on the exercise of public power by international organisations. An alternative approach is offered by Armin von Bogdandy *et al*. (eds.), *The Exercise of Public Authority by International Institutions: Advancing International Institutional Law* (Heidelberg: Springer, 2010).

16 See e.g. Bruno Simma, 'From Bilateralism to Community Interest in International Law', (1994/VI) *Recueil des Cours*, 221-384.

17 I am indebted to Léon Castellanos for intelligent discussion on this point.

Thus put, the law on State responsibility, while historically modelled on private law, does contain something of a public element, although it may be still be suggested that in doing so it comes closer to embracing a criminal law paradigm of responsibility than a public law paradigm.[18]

To make a long story short: the tasks of States, internationally, and international organisations, internationally, are different: States conclude deals with each other, and while international organisations do this too, their main task is to exercise public power. They do so over those very same States, at least to the extent that these States are members of the organisations, and they do so more generally, for instance when administering international or contested territory, providing humanitarian relief, running refugee camps, or imposing sanctions. These activities can only with great trouble be captured by the articles on the responsibility of international organisations, as these were hardly written – and, arguably, could hardly be written, given the pre-existence of rules on State responsibility – with a public law paradigm in mind.

3. The 2001 Articles on State Responsibility and 2011 Articles on the Responsibility of International Organizations

The 2001 *Articles on Responsibility of States for Internationally Wrongful Acts* (Articles on State Responsibility, hereinafter referred to as ASR) are premised on the thought that, mostly, States act on their own and incur responsibility for solo acts. Yet, it also envisages other situations, such as the situation where a State places an organ at the disposal of another State (Article 6) or where a State aids and assists in the commission of an internationally wrongful act (Article 16).

The relationship between the law on State responsibility and the responsibility of international organisations is spelled out in Article 57 of the 2001 ASR which, the Special Rapporteur suggests, should be narrowly construed.[19] Article 57 specifies that it is without prejudice to the responsibility of international organisations or the responsibility of States for the conduct of organisations. Thus, an act attributable to an international organisation will incur the responsibility of that organisation, not any of its Member States and, as Crawford explains, the same applies to what is sometimes referred to as the derivative or secondary responsibility of Member States, i.e. a responsibility resting on Member States to atone for the acts of their organisation.[20] What Article 57 does not cover, as a matter of course, is the responsibility of States for their own acts, even if performed in conjunction with the acts of an international

18 A more fully developed attempt to introduce a criminal law paradigm, by introducing an article on the criminal (as opposed to delictual) responsibility of States was, however, defeated.

19 See Crawford, Articles on State Responsibility, at 311.

20 This was a serious issue when the International Tin Council collapsed. For discussion, see Klabbers, An Introduction, 276-279.

organisation. Also of relevance is Article 47 ASR, which acknowledges the possibility of a plurality of States being held responsible; this might apply when States act together but do not do so through an international organisation.[21]

One of the difficulties underlying the *(Draft) Articles on the Responsibility of International Organizations* as adopted by the ILC in 2011 (usually abbreviated as ARIO[22]) relates to the conceptualisation of the relationship between the international organisation and its Member States. After all, often enough the organisation, while deemed to have its own separate existence in law, nonetheless is both composed of Member States (who will, together, determine the organisation's policies), and will often have to act through Member States: the European Union (EU) may have a customs policy, but lacks its own customs officials, and the UN Security Council may ordain military activities, but in the absence of an UN army will have to depend on Member States to carry out those activities.

The ARIO conceptualises the relationship between international organisations and their Member States, eventually, in a variety of ways. As a general matter, organisations incur responsibility for conduct that is attributable to them.[23] Hence, Articles 6-9 specify in detail when conduct is deemed attributable to the organisation. This applies, most obviously, to acts of organs and officials of the organisation (Article 6, and even to their *ultra vires* acts, according to Article 8), but also covers acts of State organs placed at the disposal of the organisation, provided the organisation exercises effective control.[24]

In addition, Articles 14-17 address various other ways in which organisations and their Member States can be entangled. Thus, an organisation can incur responsibility for assisting a State (or other organisation) in the commission of an internationally wrongful act; or if it directs and controls a State (or other organisation) in the commission of such an act; or if it coerces a State or other organisation to commit an internationally wrongful act. These are provided for in Articles 14-16, respectively.

The more controversial article, however, has proved to be Article 17 ARIO, which envisages the situation where an organisation aims to circumvent its own obligations by ordering or authorising its Member States to commit an internationally wrongful act. This has proven controversial because it is here, in a real sense, where the promised land of international organisations is located – it relates to situations where organisations can authorise or even order their Member States to take action. On the whole, organisations

21 See Crawford, Articles on State Responsibility, at 272-275, 310.

22 Alternatively as DARIO, with the D standing for Draft.

23 A very useful discussion, slightly pre-dating the ARIO, is Pierre Klein, 'The Attribution of Acts to International Organizations', in James Crawford, Alain Pellet and Simon Olleson (eds.), *The Law of International Responsibility* (Oxford University Press, 2010), 297-315.

24 The same applies, *mutatis mutandis*, to acts of organs of other international organisations, and Article 9 allows for the possibility of organisations acknowledging others' conduct and accepting it as their own for purposes of responsibility.

can merely adopt recommendations, asking or advising their Member States to perform particular acts but not take binding decisions to this effect. This is often regarded as a shortcoming, with the few organisations that can take binding decisions seen as the model for other organisations to try and emulate. Thus, the EU (which can promulgate binding regulations and decisions) is often regarded as the highpoint in the evolution of the species, closely followed by the UN Security Council. This facility of adopting binding decisions, so many hold, is the way forward and contributes to the 'salvation of mankind', in Singh's classic phrase.[25] Hence, organisations should not be impeded in their facility for taking binding decisions, yet this is precisely what Article 17 can be seen to be doing: it makes clear that organisations can be held responsible if they take decisions that bind their Member States and those decisions are of such a nature as to violate international law.

Potential examples are not hard to come by, and might involve such practices as a decision by the EU to ban the importation of certain products, or to assume jurisdiction over activities taking place elsewhere. It might relate to a Security Council decision which ignores due process rights of individuals, or violates their right to property. Much depends, though, on which obligations can be said to rest on international organisations, for as with State responsibility, so too international organisations can only be held responsible for internationally wrongful acts, i.e. acts that violate obligations of the organisation under international law.

This raises the question as to how international organisations actually become bound by rules of international law, and that is a question which defies easy answers. The ICJ has once specified, in general terms, that organisations are bound by their own internal rules, the treaties to which they are parties, and the 'general rules of international law',[26] and in particular the latter phrase has stirred much controversy. Some see it as a reference to customary international law generally, in which case international organisations would be bound by, for example, much of the rules of international human rights law and humanitarian law.[27] Others wonder why the Court would have referred to 'general rules of international law' if it had meant to refer to the entire *corpus* of customary international law, and suggest that the Court's reference is better seen as referring to the secondary rules of the system: those on the making and application of treaties, rather than to primary rules of conduct.[28]

---

25 See Nagendra Singh, *Termination of Membership of International Organisations* (London: Stevens and Sons, 1958), at vii.

26 See *Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt*, advisory opinion [1980] ICJ Reports 73, para. 37.

27 Sophisticated versions of this argument are made by Olivier De Schutter, 'Human Rights and the Rise of International Organisation: The Logic of Sliding Scales in the Law of International Responsibility', in Jan Wouters et al. (eds.), *Accountability for Human Rights Violations by International Organisations* (Antwerp: Intersentia, 2010), 51-128, and Guglielmo Verdirame, *The UN and Human Rights: Who Guards the Guardians?* (Cambridge University Press, 2011).

28 See e.g. Klabbers, An Introduction, at 284-285.

The other two categories mentioned by the ICJ (treaties, and internal rules) are conceptually less problematic, but nonetheless not devoid of problems altogether. Clearly, international organisations are parties to very few general international conventions; the EU is the most obvious exception here.[29] As a result, it is difficult to hold organisations responsible for violations of their treaty commitments – there are not all that many.

The category of internal rules offers organisations the possibility to incorporate international legal rules in its internal documents, but of course allow the organisation unfettered discretion as to how to incorporate international rules: as binding rules or as non-binding guidelines? Import the substance lock stock and barrel, or adapt it? Nonetheless, given the difficulties of holding organisations bound under international law, this device provides the useful service of importing some element of international law into the organisation's internal legal order.[30]

Finally, Articles 58-62 ARIO envisage different situations in which States can incur responsibility for the acts of international organisations. This applies when a State assists the organisation in the commission of a wrongful act (Article 58); if it directs and controls an organisation in the commission of a wrongful act (Article 59) or coerces the organisation into committing a wrongful act (Article 60); or if a Member State uses the organisation to circumvent its own obligations or assumes responsibility for the organisation's acts (Articles 61 and 62, respectively). The latter two points are based on the position that Member States are not generally responsible for the acts of international organisations merely by virtue of membership, a position well-entrenched in doctrine.[31]

4. Attribution and NATO

As the above suggests, one of the biggest intellectual issues bedevilling the responsibility of international organisations is the issue of attribution: organisations can only be held responsible for behaviour attributable to them.[32] How precisely this occurs is a matter

29 The EU has generated a large treaty practice, entering into treaties in its own name. For discussion, see Delano Verwey, *The European Community, the European Union and the International Law of Treaties* (The Hague: T.M.C. Asser Press, 2004). Other organisations are less active, and might have treaty relations on more mundane aspects of cooperation. Thus, the World Bank will conclude treaties with borrowing States, while the UN concludes treaties with troop-contributing States. For an early overview of the UN's practice, see Shabtai Rosenne, 'United Nations Treaty Practice', (1954/II) *Recueil des Cours*, 281-443.

30 And this, in turn, helps the organisation in question to engage in self-control which may, in some circumstances, be a viable alternative for a responsibility regime. See Jan Klabbers, 'Self-control? International Organizations and the Quest for Accountability', in Malcolm Evans and Panos Koutrakos (eds.), *The International Responsibility of the European Union: European and International Perspectives* (Oxford: Hart, 2013), 75-99.

31 See e.g. Moshe Hirsch, *The Responsibility of International Organizations toward Third Parties: Some Basic Principles* (Dodrecht: Martinus Nijhoff, 1995).

32 It is, by and large, undisputed that NATO is an international organisation possessing international legal personality. See, e.g., *Branno* v *Ministry of War* (Court of Cassation, Italy, 14 June 1954), reported in 22 ILR 756. Nonetheless, some authorities still worry; so, e.g., Joe Verhoeven, as noted in Jean d'Aspremont, 'Abuse

of some debate, but it seems clear that Member States can decide, in relevant legal instruments, to either attribute behaviour to the organisation or to refrain from doing so. With respect to NATO, several different types of situations need to be distinguished.[33] These relate mainly to military manoeuvres and the place where these are conducted.

First, there are manoeuvres involving foreign troops in peacetime, stationed on another Member State's territory. Here, the 1951 *Status of Forces Agreement* (SOFA) applies. Article VIII, paragraph 5 of the SOFA envisages that operational damage shall be compensated for by the Member States most implicated – leaving NATO itself out of the firing line.[34] In other words, an act of NATO is deemed to be an act of certain Member States. This qualification applies within NATO and need not be accepted elsewhere: a non-Member State remains free to hold NATO as such responsible and go to court to this effect. Chances are, however, that such will remain fruitless: the provision creates a strong presumption in favour of Member State responsibility, and in particular Member State liability.[35]

Second, there is the behaviour of NATO officials, working for one of NATO's military headquarters (or the acts of headquarters), which all have their own legal personality.[36] Schmalenbach observes[37] that the same rule is *mutatis mutandis* applicable: responsibility may rest on the Headquarters concerned, but liability will be assigned to the sending Member State.[38]

Third, since 1995 and the then newly-created 'Partnership for Peace' programme, military manoeuvres can also take place in States that are not members of NATO. This provides in its opening article that unless otherwise agreed, the provisions of the 1951 SOFA shall apply, and therewith also Article VIII SOFA.

Schmalenbach concludes that the regime on responsibility in peacetime by and large follows military command structures: typically, under Article VIII SOFA (in its diverse

of the Legal Personality of International Organizations and the Responsibility of Member States', (2007) 4 *International Organizations Law Review*, 91-119, at 93, note 6.

33 This follows Kirsten Schmalenbach, *Die Haftung internationaler Organisationen* (Frankfurt am Main: Peter Lang, 2004), 537-539.

34 This has given rise to some litigation in France involving traffic accidents caused by US servicemen, with the courts holding that the partiers decided to set up a pragmatic system for handling claims, treating foreign servicemen as if they were citizens of the receiving State for these purposes. See *Caisse Primaire et Caisse Régionale de Sécurité Sociale de Thionville* v *Agent Judiciare de Trésor*, Colmar Court of Appeal, 1 March 1961, and *Agent Judiciaire de Trésor Public* v *Caisse Primaire de Sécurité Sociale de la Charente-Maritime et Range*, Poitiers Court of Appel, 24 October 1961, reported in 49 ILR 498 and 500, respectively.

35 In theoretical terms, the provision distributes liabilities without bothering too much about responsibility. I understand liability in this context to refer to a legal duty to provide compensation.

36 See *Mazzanti* v *HAFSE and Ministry of Defence* (Tribunal of Florence, Italy, 2 January 1954), reported in 22 ILR 758.

37 See Schmalenbach, Die Haftung, at 539.

38 The matter is governed by the 1952 *Paris Protocol on the Status of International Military Headquarters set up Pursuant to the North Atlantic Treaty*, Article VI of which contains a complicated *renvoi* to Article VIII of the NATO SOFA.

settings), liability will follow whoever is in command, and that seems to make eminent practical sense.[39]

In principle, it would also be possible for a Member State to distribute liabilities in advance whenever an international organisation contemplates the use of military force – if they ever get round to reflecting on issues of responsibility or liability. If speedy action is taken in urgent situations, this may not be the case; if action is taken following lengthy and protracted negotiations, however, a responsibility scheme may be set up. The latter would seem to apply to NATO's involvement in the conflict in Yugoslavia after 1995: the *Dayton Agreement* (concluded between various factions in Bosnia and Herzegovina and also involving Croatia and the Federal Republic of Yugoslavia) envisaged the creation of an Implementation Force – IFOR – following a Security Council resolution, and already envisaged that NATO might establish such an IFOR, and that non-NATO Member States might contribute. The relevant Security Council resolution would be adopted a day later in the form of resolution 1031. Reportedly, IFOR has concluded agreements with Bosnia, Croatia and Serbia concerning the handling of claims, characterized by the principle that those should be dealt with, at first instance, at the level of the sending State.[40]

The International Security Assistance Force (ISAF) in Afghanistan, set up in 2001, with official NATO involvement since 2003, excludes the liability of ISAF and its staff. Formally, claims must be addressed to Afghanistan's interim government and then submitted to ISAF; in practice, partly due to lack of functioning of the interim administration, claims are invariably addressed to the sending State of the individuals considered responsible; it is this sending State which determines whether the claim is merited and which, on occasion, compensates on an *ex gratia* basis. While ISAF is seen as a NATO operation and directed on behalf of NATO, nonetheless NATO does not seem to incur responsibility in its own right.[41] This, so it has been suggested, reflects a long-standing practice: Klein concludes that practice reveals 'that it is the Member States, and not NATO as such, that have had to answer for the consequences of wrongful acts committed in the course of operations undertaken by the Organisation.'[42]

NATO structures have come before international tribunals on several occasions. The ICJ was seized following the humanitarian intervention over Kosovo, with Serbia suing ten individual NATO Member States for unlawful use of force. The Court dismissed all ten cases, largely for lack of jurisdiction, and therewith forfeited a unique opportunity

39 See Schmalenbach, Die Haftung, at 539.

40 *Ibid.*, at 558.

41 *Ibid.*, at 562-3.

42 See Klein, The Attribution, at 302, referring to the *Dayton Agreement* as well as to the *ex gratia* payment to China by the US following the bombing of the Chinese embassy in Belgrade during a NATO operation.

to shed light on the complicated relationship between international organisations and their Member States.[43]

That relationship again came before the Court in a somewhat surprising manner in 2011, in a case involving the Former Yugoslav Republic of Macedonia (FYROM) and Greece. After Yugoslavia's dissolution, a dispute ensued between Greece and FYROM concerning the use of the name Macedonia, which both parties suggest has a historical bearing on their national identities. In 1995, they concluded an interim agreement in which Greece promised not to block FYROM's applications for membership of various international organisations except in certain limited circumstances. When NATO resolved unanimously, in 2008, not to invite FYROM for membership, FYROM brought a case against Greece.

One of Greece's arguments on jurisdiction was that the impugned conduct was conduct of NATO, and could not be attributed to Greece. Hence, the Court would lack jurisdiction. In a variation, Greece argued that any judgment would automatically also affect all other NATO Member States, and thus the *Monetary Gold* principle would prevent the Court from exercising jurisdiction.[44] The Court, however, begged to differ, arguing that at issue was whether or not Greece had violated its commitments under the bilateral 1995 Interim Accord; the case did not concern the legality of NATO or of NATO's Member States in deciding not to invite FYROM to accession, but merely whether Greece's own conduct had been wrongful under the Interim Accord. Likewise, Greece could not rely on the *Monetary Gold* principle since Greece's behaviour could be assessed independently of NATO's decision.[45] In the end, the Court held that Greece had violated its own obligation under the 1995 Interim Accord, and managed to do so without delving into the relationship between Greece as a Member State, and NATO.[46]

Perhaps more pertinent cases have come before the European Court of Human Rights (ECHR). For instance, in *Bankovic*, a number of Serbians complained before the ECHR about possible human rights violations committed by a number of States acting

---

43 Then again, Klein observes that in their substantive arguments, the States concerned hardly even tried to shield themselves by referring to NATO's separate identity and thus, possibly, responsibility. This strengthens the suggestion, he argues, that in practice the Member States of NATO assume responsibility for NATO activities: 'the mere fact that an international organization is implicated in a specific activity does not suffice for any wrongful acts committed in the course of that activity to be *ipso facto* attributed to it.' Klein, The Attribution, at 303.

44 Under the *Monetary Gold* principle, the Court would be barred from deciding a case if doing so would involve an assessment of the legality of other States' behaviour without the necessary jurisdictional link. See *Case of the Monetary Gold Removed from Rome in 1943* (Italy v France, United Kingdom and United States of America), preliminary question [1954] ICJ Reports 19.

45 See *Application of the Interim Accord of 13 September 1995* (The Former Yugoslav Republic of Macedonia v Greece), judgment of 5 December 2011, paras. 42 and 43.

46 On some level it could perhaps be argued that by insisting on Greece's own obligations, the Court ignored the circumstance that Greece was acting not entirely on its own but as a member of NATO, but this critique merely reproduces the complicated nature of international organisations as both creatures of States and as entities in their own right. The conceptual issue is well fleshed-out in Brölmann, The Institutional Veil.

on the territory of the former Yugoslavia during the Yugoslav conflict. Before the Court, France, one of the States complained against, argued that the actions were not attributable to France (or other States, presumably), but rather to NATO, which it held to be a separate entity with separate legal personality under international law.[47] Some other governments argued that, regardless of attribution concerns, at the very least the US, Canada and NATO were involved in the actions; yet, none of these were parties to the *European Convention on Human Rights* (European Convention), and it would be unfair to single out certain States only (in such a case of collective action) just because they were parties to the European Convention.[48] In the end, the Court declared the case inadmissible, probably largely for the reason that Yugoslavia had never been a party to the Convention and therewith had remained outside the *espace juridique* created by the Convention.[49] It never got round to discussing the issues relating to attribution of behaviour to an international organisation.

By contrast, the Court did address such issues in *Behrami and Saramati*, and did so in a most controversial manner. Mr Behrami went to Court complaining against France that his sons has fallen victim to UN Interim Administration Mission in Kosovo (UNMIK) inaction in Kosovo (in particular the failure to clean up landmines),[50] whereas Mr Saramati had been detained by (NATO-led) Kosovo Force (KFOR) on suspicion of attempted murder and possession of an illegal weapon, and brought a claim against France, Germany and Norway. The States concerned claimed that the impugned acts had taken place outside their jurisdiction, but the Court did not follow up on the argument. Instead, the Court started by looking into the question of whether the impugned acts could be attributed to the UN, and found that both KFOR and UNMIK ultimately acted on the authorisation of the Security Council, and hence the impugned acts were attributable to the UN. As the UN is not a party to the European Convention, the Court found that it lacked jurisdiction *ratione personae* and declared the case inadmissible.

The *Behrami and Saramati* decision was, and is, considered highly controversial. On one level (and the Court anticipated as much, given its analysis of the relationship between UN and human rights law), it can be read as subordinating human rights protection to the exigencies of global peace and security or, less charitably, as 'selling out' human rights.

---

47 See *Bankovic and others* v *Belgium and others* (Application no. 52207/99), admissibility decision, European Court of Human Rights, 12 December 2001, para. 32.

48 *Ibid*., para. 31.

49 *Ibid*., paras. 79 and 80.

50 Actually, this was part of the Court's conclusion; the applicants themselves thought de-mining was the responsibility of KFOR rather than UNMIK. See *Behrami and Behrami* v *France* and *Saramati* v *France and others* (application no. 71421/01), admissibility decision, European Court of Human Rights, 2 May 2007, paras. 123-126.

A more sophisticated form of criticism, however, relates to the Court's methodology. As several observers have pointed out,[51] the Court seemed to deduce from the circumstance that behaviour was ultimately attributable to the UN that therefore the UN was the only entity to be held responsible, and refused to investigate whether, even given UN responsibility, there would be some room left for responsibility of the Member States concerned or, in the case of Saramati, whether there was some responsibility to be carried also by KFOR. The general gist of these comments is that responsibility can be shared by various actors and need not be exclusive. While sharing responsibility may create other issues (for example, 'who is responsible for which part of the activity' is a perennial question[52]), it does not automatically follow that responsibility is or should be exclusive.[53]

5. A Thought Experiment

The extent to which cyber operations give rise to discrete legal issues is not entirely clear. There are, it seems, three schools of thought.[54] According to the first, cyber operations are merely a new technique of warfare, and thus not in need of specific regulation. Or, if specific regulation is needed, it is to adapt the *jus in bello*; the *jus ad bellum*, however, remains unaffected. A second group of authors feels that there is a need to subject governmental cyber operations to a specific treaty, which would probably involve both *jus ad bellum* and *jus in bello*.[55] Third, some hold that without prejudice to the *jus in bello*, the current *jus ad bellum* needs to be re-interpreted in order to do justice to the new phenomenon of cyber.

For present purposes, this discussion does not seem all that relevant – as suggested above, the current chapter works on the presumption that while the primary rules of international law may need to be adapted to accommodate cyber activities, this does not hold true with respect to the secondary rules. What does matter for present purposes, however, is what happens when an armed attack by cyber means occurs, or when NATO acts in collective self-defence, regardless of the precise definitions of armed attack or self-defence.[56] Likewise what matters is, if the Security Council should authorise a

51 See, e.g., Verdirame, The UN and Human Rights, and Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press, 2011).

52 Public administration scholars have called this the 'problem of the many hands'; see Mark Bovens, *The Quest for Accountability* (Cambridge University Press, 1998).

53 There are reasons however not to exaggerate the relevance of *Behrami and Saramati*: it concerned a decision on admissibility (and as such ought not to be seen as having subordinated human rights), and much of the reasoning revolved around the special character of the UN, and might thus not easily be applied to other organisations. See Klabbers, An Introduction, at 280-281.

54 I am indebted to Lianne Boer for useful discussion on this point.

55 Otherwise the second group would collapse into the first.

56 On such issues, see e.g. Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', (1999) 37 *Columbia Journal of Transnational Law*, 885-937; Katharina Ziolkowski, '*Ius ad Bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of

military operation led by NATO 'by all means necessary', including cyber means, what are the precise modalities of the cyber activities conducted, rather than whether it meets some definition or other. Put differently, the discussion of different means of military operations and whether or not this forces a re-thinking of *jus in bello* and *jus ad bellum* is of relevance when the task is to assess whether an actor's acts violate international law and findings of initial responsibility, but seems to have little direct bearing on distribution of responsibility or liability.[57]

Nonetheless, it may be useful to explore the way the law on responsibility operates in cases of cyber operations, and it might be illuminating to do so by sketching possible scenarios going to the heart of NATO's task: the exercise of self-defence. At least four different scenarios may be distinguished. First, NATO itself may be under attack, and therewith strike back claiming a right of self-defence. Second, one of NATO's Member States may be under attack and exercise its individual right to self-defence. Third, one or more of NATO's Member States may be under attack, and several of these may exercise a right to defend themselves collectively. And fourth, it might be the case that NATO itself would conduct military operations outside of the realm of collective self-defence, including by cyber attacks.[58]

NATO is the textbook example of a self-defence organisation,[59] with Article 5 of its constituent treaty providing that an attack against one Member State shall be regarded as an attack against all, triggering a possible collective exercise of self-defence. It has been scathingly – if accurately – remarked that Article 5 contains a clear 'element of non-commitment in the commitment'[60] (in that the possibility to achieve collective self-defence is optional rather than compulsory), and it would seem that the provision has been invoked only once in all of NATO's existence, and that was right after the attacks on New York's World Trade Center on 11 September 2001.

Scenario 1: NATO Itself is under (Cyber) Attack

It is, arguably, not all that far-fetched to suppose that like any complex bureaucratic installation, NATO too might be vulnerable to a cyber attack showing the quality of

Force', in C. Czosseck, R. Ottis and K. Ziolkowski (eds.), *2012 4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012), 295-309, and Lianne Boer, 'Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace', (2013) 5/3 *Amsterdam Law Forum*, 4-18.

57 There are possible caveats here. Self-defence, for instance, must remain proportional to the act of force giving rise to it, so at this level the precise definition of armed attack and the precise definition of what activates self-defence may become of relevance.

58 Other scenarios may become a bit too far-fetched. Thus, it might happen (hypothetically, of course) that one of NATO's Member States commits aggression triggering someone else's right to self-defence, but in such a case the connection with NATO seems, at best, optional: possibly the self-defence of that other might trigger the collective self-defence under NATO's aegis, but might also not do so.

59 Quite literally so, with its institutional aspects making it more than a traditional alliance: see, e.g. Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace*, 2d ed. (New York: Alfred Knopf, 1955), 495-496.

60 See Michael J. Glennon, *Constitutional Diplomacy* (Princeton University Press, 1990), at 214.

an armed attack in the meaning of Article 51 of the *Charter of the United Nations* (UN Charter). NATO Headquarters in Brussels, or one of its Supreme or Regional Headquarters, may be on the receiving end of a computer network attack, perhaps in particular by the transmission of viruses.[61] If this is the case, issues of responsibility on the part of NATO do not arise: under Article 21 ARIO, the 'wrongfulness of an act of an international organisation is precluded if and to the extent that the act constitutes a lawful measure of self-defence under international law.' According to the ILC's commentary, this may also cover situations where an operational mission is under attack.[62]

The presumption underlying Article 21 ARIO seems to be that it is the organisation itself that acts in self-defence. If so, it leaves unsaid whether a Member State can act in defence of the organisation; one may imagine a situation where the technological prowess of one of the Member States is relied on to repel an attack on NATO Headquarters. In such a situation, presumably the right to engage in collective self-defence may apply, provided the organisation asks the technologically advanced State to help repel the attack.[63]

A variation on this scenario would entail the situation where a NATO mission, consisting of national contingents, were under attack. In such a case, it is undisputed that NATO can exercise self-defence, and a strong case can be made that the same applies to the national contingent or contingents involved. These contingents, after all, remain organs of their sending States.[64]

Should the attack be a cyber attack, and should it be repelled by NATO officials without Member State assistance, and should in doing so NATO transgress the limits of lawfulness, then NATO itself would incur responsibility under international law: the unlawful acts would be acts committed by the organisation.[65] Such a scenario is not completely unimaginable: one could think of NATO computer experts repelling a cyber attack and doing so overzealously, going beyond the limits of proportionality and necessity which by definition qualify the right to self-defence.

---

61 There is a thin line between cyber crimes and cyber attacks. The former would include, arguably, such things as copyright violations on the internet or gaining unauthorised access to data. See generally Pia Palojärvi, *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict* (Helsinki: Erik Castrén Institute, 2009).

62 See International Law Commission, *Draft Articles on the Responsibility of International Organizations, with Commentaries* (New York: United Nations, 2011), at 46. Note that Article 21 is drafted, it seems, exclusively with the UN in mind.

63 This derives from the *Nicaragua* case, and there seems to be no good reason to preclude the possibility of collective self-defence when the victim of the armed attack is an international organisation. See *Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua v USA), Merits, [1986] ICJ Reports 14, paras. 232-234.

64 See Paolo Palchetti, 'Armed Attack against the Military Force of an International Organization and Use of Force in Self-defence by a Troop-Contributing State: A Tentative Legal Assessment of an Unlikely Scenario', (2010) 7 *International Organizations Law Review*, 241-260.

65 This does not preclude NATO and its Member States from distributing liabilities in the agreement setting up the mission concerned.

Scenario 2: Individual Self-Defence

In this scenario, responsibility again creates few problems, at least as far as attribution goes. State A is under attack, and acts in self-defence without asking for anyone's assistance, and without NATO's other Member States invoking Article 5 of the *North Atlantic Treaty*. Under Article 21 ASR, the wrongfulness of the self-defence is precluded as long as the self-defence meets with the conditions of the UN Charter and can be considered lawful. The latter means, in particular, that it respects the requirements of necessity and proportionality. Still, as Crawford observes, some obligations remain in force, regardless of whether self-defence is exercised, and this applies in particular to humanitarian law and human rights obligations. Hence, self-defence does not necessarily excuse all behaviour. That said, this scenario does not give rise to issues of attribution, for the simple reason that no plurality of acts is envisaged.

Scenario 3: Collective Self-Defence through NATO

In this scenario issues of attribution may come to play a prominent role. One option is for the States concerned, engaged in the exercise of collective self-defence, to do so without involving NATO at all, but deriving the right to do so from Article 5 of the *North Atlantic Treaty*. If NATO *qua* institution is not implicated (and nothing in its constituent treaty suggests that it needs to be implicated)[66], then the acts of the Member States are best seen as acts by a plurality of States. In this case then, the responsibility of NATO is not at issue; instead, Article 47 ASR applies, suggesting that each individual State participating remains responsible for its own contribution, but that joint responsibility may also occur.[67] Either way, to the extent that the self-defence remains lawful, it functions as a circumstance precluding wrongfulness under Article 21 ASR.

It may also be the case that NATO will be implicated in one way or another. Thus, there is the possibility (hypothetical, at any rate) of NATO deciding to authorise an act of collective self-defence. This would have the potential to bring the responsibility of NATO into play, should the act of self-defence exceed the boundaries of lawfulness, but much will depend on the precise modalities: if NATO merely authorises the action but does not turn it into a NATO operation or does not order its Member States into action with binding force, then matters are unclear. The ARIO does not seem to address the issue of authorised action explicitly, although it would seem, based on the ILC's commentary, that its Article 7 comes closest. Under Article 7, conduct by State organs placed at the disposal of an organisation shall be considered acts of the organisation, at least as long as the organisation exercises effective control. The commentary relies

66 This taps into a possible distinction between the *North Atlantic Treaty* and the organisation set up on the basis of that treaty. It has long been recognized that such a distinction may exist and may have legal consequences (thus allowing, e.g., for withdrawal from an organisation while remaining a party to its foundational instrument), but little work has been done to elaborate. One possible illustration resides in France's partial withdrawal from NATO in the 1960s: see Klabbers, An Introduction, at 112.

67 See Crawford, Articles on State Responsibility, at 272.

heavily on the approach developed by the ECHR in *Behrami and Saramati*, as discussed above. Yet, as noted, *Behrami and Saramati* is vulnerable to criticism, and has been considered to go against the regular practice of both the UN and NATO, for under regular practice the Member States retain responsibility.[68] Either way, in cases of merely authorised action, it is by no means clear that the organisation can be said to exercise effective control.[69]

The one article addressing scenarios of authorisation is Article 17 ARIO, but this is a curious provision, premised on the idea that the organisation would wilfully authorise (or order) its Member States into the commission of wrongful acts. It is, in other words, premised on the sort of bad faith that would seem to be rare in practice. While it can easily be acknowledged that organisations can and do commit wrongful acts, it seems doubtful that they would do so intentionally, in order to circumvent an obligation resting on the organisation itself. At the very least the provision opens up a host of interpretative issues. For instance, should NATO authorise its Member States to violate humanitarian law in the course of collective self-defence, it ought to incur some responsibility, but does one really need to show an intention to circumvent?[70] The ILC Commentary suggests as much,[71] but it would seem that the far more likely scenario is that of an organisation authorising behaviour which, upon reflection, may constitute a wrongful act, but was not authorised with the intention to circumvent.[72]

Should NATO go further and turn the act of self-defence into NATO action (for instance by launching a NATO-led mission) then, arguably, the applicability of Article 7 is more plausible, for there is a greater chance that in such circumstances NATO does indeed exercise effective control. This applies even if the troops are placed at NATO's disposal by its Member States, although much may depend on precise conditions on the battlefield (if that term can meaningfully be used in situations of cyber operations). After all, effective control is not a formal matter, but can shift over the course of an operation, as the case law makes clear.[73]

---

68 See Klein, The Attribution, at 302-303.

69 Partly for this reason, it has been argued (although perhaps limited to the UN) that the better view would be to regard situation in which troops are placed at the disposal of an organisation to give rise to a rebuttable presumption that responsibility will rest with the organisation, following Article 6 ARIO. See Aurel Sari, 'UN Peacekeeping Operations and Article 7 ARIO: The Missing Link', (2012) 9 *International Organizations Law Review*, 77-85.

70 Critical on this point also Blokker, A Mid-Term Review, at 324.

71 'The term "circumvention" implies an intention on the part of the international organization to take advantage of the separate legal personality of its members in order to avoid compliance with an international obligation.' See ILC, Draft Articles, at 41.

72 The Commentary also makes clear that no organisational responsibility arises for other violations that may occur.

73 The ILC commentary refers, e.g., to an unpublished Belgian court decision in *Mukeshimana-Ngulinzira and others* v *Belgian state and others* (see ILC, Draft Articles, at 22) while reference may also be made to the decision of the Dutch Supreme Court in *Nuhanovic* (referred to in note 4 above).

Scenario 4: NATO Cyber Operation without Member States' Involvement

While NATO was not created with the purpose of leading military operations in circumstances other than self-defence, practice suggests that since the end of the Cold War, it has transformed itself into an organisation that can also operate out of area and, what is more, an entity that also has the competence to engage in action beyond strict self-defence.[74] The intervention in Kosovo, initially deemed by some to be illegal but morally justifiable,[75] is but a prime example. Other examples are the multitude of NATO-led military operations conducted under the mandate of the UN Security Council (Chapter VII of the UN Charter). Again, what matters here is how the operations take place. With kinetic operations, it seems almost impossible for NATO to engage in action without involving the resources of Member States; as a result, much of what was discussed above under scenario 3 would apply here as well.

Things might be different though with cyber operations, as it seems technically possible for a small team of computer experts to launch a computer network attack. Here then, supposing that the experts concerned are all NATO employed 'international civilians' or contracted specialists, the responsibility will solely rest with NATO: the conduct of an official of an international organisation 'shall be considered an act of that organisation under international law' in the formulation of Article 6 ARIO. This applies if the officials act in the performance of their functions, but also if they exceed their authority or go against instructions. The latter follows from Article 8 ARIO, dealing with *ultra vires* acts and containing the basic principle that the organisation retains responsibility. The commentary to that article makes clear, furthermore, that while off-duty conduct of officials may remain beyond the responsibility of the organisation, nonetheless it might come within the realm of the organisation's responsibility if the obligation breached is a general obligation of prevention.[76]

Should the computer experts concerned be partly employed by NATO as 'international civilians' or contracted by the organisation, and partly be State officials, employees or contractors seconded to NATO by one or more of the Member States, it would seem that Article 48 ARIO may apply. Much like Article 47 ASR, this provides for plural responsibility, although by contrast with Article 47 ASR it shuns the use of the word 'plural'.

The above scenarios seem to suggest that the circumstances in which NATO can be held responsible are fairly limited, and much will depend on the degree of control exercised by NATO. It is arguable that this degree of control can increase dramatically in the

74 The development is carefully tracked in Stefan Bölingen, *Die Transformation der NATO im Spiegel der Vertragsentwicklung: Zwischen sicherheitspolitischen Herausforderungen und völkerrechtlicher Legitimität* (Saarbrücken: VDM Verlag, 2007).

75 See e.g. Bruno Simma, 'NATO, the UN, and the Use of Force: Legal Aspects', (1999) 10 *European Journal of International Law*, 1-22.

76 See ILC, Draft Articles, at 29.

case of a computer network attack, whether engaged in by NATO or committed against NATO, simply because such cyber activity does not require the involvement of many personnel or troops or weapons. While it is almost unthinkable that NATO could engage in kinetic armed activities without having to rely on its Member States, it is by no means impossible to imagine NATO being the sole agent with regard to the exercise of a cyber operation previously decided upon by its Member States. It is here then that cyber operations may make a legal difference even with respect to issues of responsibility, although, strictly speaking, more on the practical level than on the level of the law: since it may practically speaking be possible for NATO to engage in solo acts, the chances of it incurring responsibility might increase.

As a more general point, it might be useful for international lawyers to further develop the (thus far largely intuitive) distinction between responsibility and liability. As the above discussion suggests, the standing practice seems to be to hold Member States responsible even when conduct can in whole or in part be attributed to NATO (or to an international organisation generally). If so, the use of the term responsibility for both situations is awkward – it might be more transparent to hold the organisation responsible but the Member States liable, if there is an agreement to this effect in place.

6. By Way of Conclusion

It goes without saying that much of the above is hypothetical and simplified. The law on self-defence, for example, is kept simple, without any regard for niceties involving the identity of the attackers (whether a State, another international organisation, a liberation movement, or a terrorist group), and without any regard for the complexities of how to identify an armed attack: do minor boundary infractions already qualify? Is anticipatory self-defence a possibility, and if so, does a pre-emptive strike in accordance with the Bush doctrine also qualify?[77] The scenarios are stripped down to their bare essences for heuristic purposes, but it is useful to realise that in real life, such bare essence scenarios will be rare, perhaps non-existent.

There is also an obvious element of speculation involved in the above discussion. After all, the degree to which ARIO reflects standing practices and may even be said to represent customary international law is debatable; it may turn out to be the case that the practice of international organisations will depart from the rules as formulated in ARIO. By contrast to the ASR, the authority of ARIO still needs to be established, and it may be the case, as noted before, that ARIO contains too many ambivalences to become authoritative, not because of any technical flaw but simply because of the ambivalences inherent in the law of international organisations.[78]

---

77 For further discussion, see Klabbers, International Law, at 192-196.

78 See generally Klabbers, An Introduction.

If so, however, at least on one point the utility of ARIO may be highlighted: the relations involved in military operations (be they cyber operations or other varieties) tend to be located mostly on the level of international relations – i.e. precisely where the private law paradigm underlying much of the responsibility regime is most appropriate. Put differently: to a large extent, military activities between NATO and its Members and some other entity are different in nature from, say, the imposition of individual sanctions by the Security Council or the administration of territory by UNMIK. The latter are exercises of public power in a way that the former is not – here a public law paradigm of responsibility, focusing on proper administration, judicial review and the like, would be more appropriate. Still, because military operations do not involve the exercise of public power in quite the same way, the private law paradigm underlying ARIO need not be detrimental.

Most importantly perhaps, the above examples are, almost inevitably, examples of what moral philosophers tend to refer to as ideal theory: in the messy real-life world, situations are inevitably more complex than the law of responsibility can represent them.[79] For it is a characteristic of the law of responsibility that it takes a slice out of life, de-contextualises it to the fullest extent possible, and then apportions blame and liabilities for past conduct.[80] As a result, it becomes important to figure out how the slice is identified, and perhaps even more so by whom. In other words, the framing of the issue is of great relevance, in the law of responsibility as well as elsewhere.[81]

That is not to say that the law of responsibility is useless. In fact, it serves several useful functions, not just when it comes to assigning blame and liability, but also in the thought that to be held responsible implies being taken seriously as an actor.[82] Moreover, in the post-positivist setting of global governance, where it has become next-to-impossible to distinguish between law and non-law, and where informal and soft agreements compete for application with hard and fast treaty rules, somehow a responsibility regime comes across as the final island of certainty in an ocean of doubt: it may be impossible to tell whether entity X is legally bound to behave in a certain manner, but if it really does nasty things, an argument to hold it responsible can usually be found. Therewith, responsibility doctrine has come to replace source doctrine in international legal discourse, and is thus of considerable political relevance, arguably more so than its legal

79 On the relevance for any normative thinking (and this would include thinking on responsibility) to situate itself in the real world, however precisely defined, see Raymond Geuss, *Philosophy and Real Politics* (Princeton University Press, 2008).

80 A more forward-looking model is developed under the heading of 'social connection model' by Iris Marion Young, *Responsibility for Justice* (Oxford University Press, 2011). See also Elnoor Ebrahim and Edward Weisband (eds.), *Global Accountabilities: Participation, Pluralism, and Public Ethics* (Cambridge University Press, 2007).

81 See more generally, e.g., Nancy Fraser, *Scales of Justice: Reimagining Political Space in a Globalizing World* (New York: Columbia University Press, 2009).

82 As noted by Tony Honoré, *Responsibility and Fault* (Oxford: Hart, 1999), at 10.

function alone would, strictly speaking, justify.[83] Either way though, as generations of international lawyers have come to realise, no miracles should be expected from responsibility regimes, and that applies both to traditional military operations and to cyber operations.

[83] The attentive reader will note that all this implies that the requirement of the wrongful act, so central to the international law of responsibility, in practice tends to be considerably relaxed. For a brief discussion along these lines, see Jan Klabbers, 'Back to Front: Positivism, Constitutionalism, and Accountability', in Jean d'Aspremont and Jörg Kammerhofer (eds.), *International Legal Positivism in a Post-modern World* (Cambridge University Press, forthcoming).

Part III

State Interaction and Counteraction in Cyberspace

*Heli Tiirmaa-Klaar**

Cyber Diplomacy: Agenda, Challenges and Mission

1. Introduction to Cyber Diplomacy – An Agenda for a Rising International Relations Sub-discipline

Many International Relations students and career diplomats are faced with a new subject called international cyber issues, or cyber diplomacy. It includes information and communication technology (ICT) policy, international cyber security, bilateral cyber dialogues, development policy, internet issues, human rights in the cyber era, trade and intellectual property issues, and many other policy issues. Terms and concepts of what constitutes cyber diplomacy are still shifting, and the subject develops rapidly.

This new stream of work for diplomats has opened up a whole new avenue for inter-state relations, comprising a wide array of foreign policy instruments. It also includes a substantial number of different domestic and foreign stakeholders. Therefore, new routine coordination tasks have emerged for Ministries of Foreign Affairs (MFAs) that require comprehensive knowledge on information technology (IT) developments, computer and network security, internet governance, international security, cyber crime, cyber intelligence, etc. Most of these subjects are not yet thought of in diplomatic academies or international affairs schools. At the same time, diplomats should learn quickly to speak 'cyber' as this issue evolves rapidly. It is especially important now, when more states are appointing senior officials to steer this new area of international relations. In the future it will be very important to have a new generation of capable and trained diplomats to take the international cyber agenda forward. The present chapter intends to fill some of these gaps, and offers a practitioner's view on the major challenges and requirements of this policy area, which new generations of diplomats will be likely to cross in their career paths.

If practitioners in the field were asked what constitutes cyber diplomacy, they would likely offer very different views. Some will assert that it is mainly freedom of expression online, others would state that it should be the global fight against cyber crime, and yet others would say that we need to agree on rules for cyber warfare. The reality is that a successful cyber diplomat should have a basic knowledge of many parallel subjects as, in real life situations, they must make decisions informed by different foreign policy aspects.

* This chapter represents the personal opinion of the author and should not be attributed to any organisation with which she is affiliated.

As we are still in a very early stage of shaping cyber foreign policy, few MFAs have a special cyber office. In the majority of the MFAs, cyber aspects are being mainstreamed into daily work on human rights, international security, transnational threats and other issues, even if there is no special cyber unit established. If states would like to cover all relevant cyber aspects, they need a good team of cyber diplomats. A specialised office with knowledge of cyber issues is an advantage, but it is also important to have sufficient horizontal coordination between geographical and thematic diplomats on cyber issues. An ideal horizontal cyber coordination structure should include human rights, international security, intelligence analysis, global threat issues, and relevant geographical and multilateral diplomats in foreign ministries.

It is not easy to prioritise the different international cyber issues. A central traditional element of foreign policy has been the protection of basic rights and freedoms, and it would make sense to start from here. In liberal democracies, one of the most central elements of foreign policy is to promote international activities that help to defend human rights, both offline and online. The inherent tension between internet freedom and cyber security requirements has led many governments, including those of liberal democracies, to make hard choices as to how the internet technology is used to maximum effect for collective wellbeing, with a minimum infringement of fundamental rights. An increasing trend towards internet censorship and mass surveillance calls for collective action to condemn the regimes suppressing freedom of expression in new media.

Diplomats should become more involved in preserving the internet as we know it now. A free and open internet itself is not a given phenomenon, and has been challenged by many actors since its birth. The World Wide Web as a platform for communication emerged from technical communities, and became a worldwide critical infrastructure which transformed the way we connect with other people and how we think and do business. The effect of the internet as a liberating technology for many unprivileged, disconnected and uninformed social groups is tremendous, and should be preserved in its current form. The internet has been a success story because of private sector led innovation, and voluntary cooperation between non-governmental and private sector groups. A pre-condition for continued innovation will be to preserve the key role of the private sector innovation and civil society drivers in the current internet governance model. This topic should be also mainstreamed into foreign policy.

At the same time as promoting free internet and human rights online, diplomats need to cater to a very concerned law enforcement community, which sees cyber crime skyrocketing. Equally serious, and an even more concerning trend, is silent cyber espionage for industrial purposes. When designing cyber dialogues and international cyber policies, all these aspects need to be taken into account. For instance, a state cannot tailor operational cyber security cooperation with foreign partners that are known for intruding into its companies' computers and stealing their trade secrets. Or, diplomats should be hesitant in building law enforcement training programmes in states

where this know-how could be used to suppress freedom of expression or to jail anti-government bloggers.

Last but not least, all diplomats should have a basic understanding of the rules of war and conflict, as cyberspace is now deemed as a fifth warfighting domain alongside land, sea, air and space. International security concerns in cyberspace start with the fact that states are still working on the rules and norms of state behaviour in cyberspace. The first international security related cyber challenge is to achieve a common understanding as to what constitutes the parameters of state behaviour. Some very useful initiatives have contributed towards this goal, such as the United Nations Group of Governmental Experts (UN GGE) reports in 2010 and 2013, or the global Cyberspace Conference process that started in London in 2011. There is also a process underway in the Organization for Security and Co-operation in Europe (OSCE) to establish agreement on cyber security Confidence Building Measures (CBMs). Valuable inputs to the discussion have been provided also by the academic community, notably the 'Tallinn Manual'[1] regarding the applicability of international humanitarian law (IHL) in cyber warfare. These first steps in setting the norms in the 'Wild West' of cyberspace should be encouraged and mainstreamed into international security policy discussions. Significant work has been carried out in hammering out the details as to how CBMs or IHL actually should apply in cyberspace, so there is a good basis already on which to go forward.

One of the major goals for both national and international cyber policy-makers should be to mainstream cyber issues into existing policy fields, such as internal security, critical infrastructure protection, international security and human rights policies. Given the large number of domestic and international actors in the field, diplomats might find it extremely challenging to understand and participate in decision-making on cyber policies. This chapter will first illustrate the cyber security agenda that governments face nowadays. Secondly, it will describe the five major work areas where international policies can assist in responding to the growing cyber threats. An additional objective of this analysis is to show how crucial the continuous mainstreaming of cyber policies will be, and how to overcome the natural tendency of fragmentation of states' cyber projects into several silos. To have a successful cyber foreign policy, diplomats need to be plugged into structured, national cyber coordination.

2. The Fifth Domain and Policy-Making Challenges

Ever since William Herschel encountered infrared light in 1800, the discovery of electromagnetic waves has facilitated technological progress. The development of optical fibre for telecommunications and computer technology opened up a new era that we now call the ICT revolution. We live now in an era which is witnessing a huge

[1] 'Tallinn Manual on the International Law Applicable to Cyber Warfare' ed. Michael Schmitt (Cambridge University Press, 2013).

paradigm shift in how the ICT revolution and technology governance will be viewed in the future. While initially the ICT revolution was only viewed positively, and only useful for economic growth, the paradigm shift of in the 1990s occurred when the spread of malware started to be a real global problem for industries and governments. The decade of 2000-2010 will probably be called a breaking point in future history textbooks, when mankind saw cyber attacks supporting military advances and cyber tools were first used for the purpose of disruption and destruction of physical infrastructure.

In the early years of ICT technology and the internet, no one could predict that this new technological support function would become a critical backbone infrastructure that underpins all economies and societies. There are certain milestones as to how the internet and ICT developed into a global critical platform, with the introduction of the domain name system (DNS) and commercialisation of the internet, the explosion of software products, the growth of the online economy and other events, all marking an ever-growing dependence on ICT. All private sector led ICT development was oriented towards supporting business continuity, guaranteeing quick access to information and fast connectivity. Security was often an afterthought while companies and governments built up complex information systems. Now ICT security specialists have identified that, because of the complexity of the ICT architecture in the majority of our organisations, 100% security is impossible to achieve in any of these systems. The best one can do nowadays is to quickly detect unwelcome visitors in computer networks, since there is always a possibility of breaking the codes and getting unauthorised access to any computer. Specialists say that prevention and defence have largely failed, and detection is now the primary focus of computer security professionals. While the cure for this problem should be found in new technological breakthroughs and should be discussed in academic cryptographic and mathematics circles, policy-makers still operate in the current situation, where low levels of security in ICT technology are an increasingly dominant feature of this man-made domain.

However, the genie is out of the bottle and we cannot go back to stone tablets, paper rolls and typewriters. The economic growth that cyberspace facilitated still outweighs all security concerns, and cyber security policies have not yet been mainstreamed as major issues for senior national or industry leaders. Among laymen there is also a very low awareness of what cyberspace is, how much we depend on it, and what domestic policies are in place to protect the security of critical information systems.

Cyberspace does not consist only of the internet, but of different technologies, computers, phones, devices, fibre-optic cables, routers, software, etc., which are all in constant and rapid development cycles. The technology world has been able to provide fast connections and new ways to access information, and to create business opportunities. ICT technology facilitates all critical services in our societies and economies, be they energy, telecommunications, water supplies or air control systems. There are almost no critical services that do not depend on information systems nowadays, and the

penetration of information technology reaches everywhere. Even archives of medieval documents are now digitised, as well as medical files and other sensitive personal information.

Due to the complexity of technology issues, public policy-makers are still in the early stage of understanding how to steer national cyber security policies, protect industrial or governmental secrets and help law enforcement authorities to fight cyber crime. Since the vast majority of all critical cyber assets belong to the private sector, any successful national cyber policy should include close public-private partnership and horizontal coordination across industrial sectors and government departments. The national cyber policy coordination should, of course, include also the foreign and security policy community. As national cyber policies are still forming and states are often still searching for a national champion to lead cyber efforts institutionally, it is not easy for the foreign policy community to establish itself in this area. Given the international atmosphere, where every cyber security announcement must be balanced with human rights and other foreign policy concerns, diplomats must be part of states' cyber policymaking circles. All in all, diplomats should be important cyber policy drivers, the reasons for which will be explained below.

Every foreign policy professional has probably encountered the argument when facing national policy-makers that a certain field requires expert knowledge that diplomats do not have and, therefore, decisions should be made by experts in the area. This pattern might also be repeated in cyber debates, where the tradition of the national technical community and relevant line ministries driving this policy area is still strong. To help struggling diplomats, one can make a strong argument that, as cyberspace is a global critical domain for all other human activities, comprehensive policies on cyber issues require the involvement of international relations professionals. As nuclear engineers do not represent states at the non-proliferation negotiations, likewise technology experts should not drive the issue of cyber diplomacy. Similar to domestic cyber policies, where cyber aspects should be incorporated into crisis management and critical services protection, makers of foreign policy and the national security community need to learn and mainstream cyber issues into their routine work.

In order to understand and de-mystify cyberspace for policy-makers, it would be useful to conceptualise the cyber policy agenda according to the consequences of cyber infrastructure disruptions or destruction, or economic loss from cyber crime and espionage. Prevention, damage mitigation and decreasing the systematic risks in cyberspace require the involvement of the makers of foreign policy. For diplomats, the most serious concern should be to avoid possible consequences of information infrastructure disruptions or destruction at the global and regional level. One can expect that any responsible international actor aims to avoid catastrophic cyber events. Nevertheless, in theory, some cyber attacks can cause damage and harm that equals kinetic attacks. It is possible to imagine that, during a regional conflict, a 'flooding'

attack, combined with 'surgical' cyber attack or together with a physical attack on the information infrastructures, is organised in order to create economic loss in another state for political reasons. If the financial system also depends on the attacked information infrastructure, it can cause serious disruption of financial services in a region.

States with modest cyber defence capabilities have increasing concerns, because the dual use domain is becoming increasingly criminalised and militarised. The total asymmetry of the domain creates unacceptable vulnerabilities for critical private and public information systems. In future conflicts, cyber attacks can occur against a state's critical infrastructure, whether during a military conflict or not. Cyber attacks that occur during international armed conflicts will be regulated by IHL. In these situations, states should follow the respective regulations to avoid affecting the civilian population, finding proportionate methods and calculate secondary effects, to name just a few. Indeed, cyberspace has evoked new discussions on how IHL can apply. Many lawyers say there is a gap in international law as to how to regulate humanitarian aspects in a conflict when cyber attacks cause significant disruption and suffering to civilian population, but do not qualify as such as an armed conflict.

An unsolved attribution issue will add complexity to cyber events both in wartime and peacetime. Even if states agree to some norms and laws, the relative ease of using proxy actors can motivate them to opt for cyber tools. As long as states with a weak capacity of government to monitor data flows or fight cyber crime exist, the attribution issue remains. Collective work should be undertaken to diminish the number of 'cyber safe heavens'.

It will be largely up to foreign policy community to design international mechanisms for inter-state relations regarding cyberspace issues. The first task for diplomats will be to decrease the probability for misperceptions, misattribution and lack of confidence in cyber relations. Together with domestic cyber communities, diplomats should work to prevent or mitigate cyber related disruptions.

A primary issue for the national security policy community will be the protection of civilian critical infrastructure that will possibly suffer most in future conflicts. In a situation where approximately 80-90% of critical cyber infrastructure belongs to the private sector, governments should invest in national cyber resilience systems. Public-private partnerships and crisis management frameworks for cyber security should be developed as a response to the new threat landscape. The private sector has introduced some working cyber crisis management mechanisms that have been successful so far, and there should not be too much involvement of governments where the private sector covers the ground. What the foreign policy community can add is its work towards building trust between nations, creating communication channels and bringing different parties to the negotiation tables. Notably, the diplomatic community should become more aware of protecting critical civilian infrastructure worldwide. Development assistance is needed to build a broad base of civilian cyber capabilities, preventive mechanisms

and efficient crisis management that constitute the building blocks of a national cyber system. Most advanced cyber nations have already realised that the efforts of traditional militaries are insufficient in modern conflict with its extensive cyber activities. Instead, states are looking for new civilian crises management mechanisms and ways to mobilise non-state actors which might have an essential role to play in future cyber conflicts.

Most serious consequences from malicious cyber activity fall on economic actors – companies and industries in different sectors. Financial gains by cyber criminals have already mobilised the banking industry to form cyber security information sharing centres, and to invest more heavily into reputational aspects to cover the costs of cyber crime. Many other sectors experience constant intrusions and attacks nowadays, as organised crime is also moving to cyberspace. Utilities providers need extra help from states when they are probed by state-sponsored actors with considerable resources. Cyber tools are increasingly used to facilitate traditional crime. Most large companies have invested heavily in cyber protection, and have chosen to accept the risk of rising cyber crime. However, very few companies are ready to disclose the actual losses from cyber intrusions. This has a boomerang effect in the long run, since the lack of reliable data on cyber crime prevents shareholders and public policy-makers from reacting to this growing threat.

Law enforcement experts complain that there is a systemic underinvestment in the area, making it harder to fight growing organised cyber crime. As cyber crime is carried out in computer networks is hard to 'smell' or 'touch', public authorities are lagging behind in acknowledging and reacting to this new risk. In most states, law enforcement personnel are working extremely hard to keep track of spiralling cyber crime. Smaller companies suffer most as they do not have enough resources to keep their cyber defences up to date. With increasing revenues from global cyber crime, criminal actors are getting more organised, and the related economic loss will present a serious risk for governments in the long run. Governments need serious national capabilities for fighting cyber crime, which poses a threat to internal, national and economic security of all states.

None of the national mechanisms of individual states is sufficient in the case of a large-scale cyber crisis or in fighting international organised cyber crime. Addressing global cyber crime is a challenge that has clearly reached an alarming level, and should be addressed by the foreign policy community. The promotion of the Council of Europe's (CoE) *Convention on Cybercrime* should be mainstreamed into diplomatic efforts to ensure a sufficient legal framework to address cyber crime outside of the developed world.

Cyber espionage for economic purposes presents yet another challenge to governments, including diplomats. Silent transfer of intellectual property might pose the same

risk to economic prosperity as plain cyber crime.[2] It is clearly another field where diplomatic intervention is required to agree on state behaviour which establishes norms in cyberspace. Admittedly, cyber conflicts and other threat-centred issues are closer to diplomats who are trained to deal with matters of security policy. However, diplomats should also understand the protection of intellectual property online and some other cyber related economic issues. Trade experts are increasingly faced with unfair market barriers that some states have raised by setting ICT product standards justified by national security. These sometimes disproportionate standards are used to block market access to foreign manufacturers. Again, diplomats should be informed by trade negotiations on this issue.

Current cyber developments open up another area undiscovered by diplomats, namely internet governance. This complex field of initiatives and forums belongs mainly to technologists. The foreign policy community's attention to this area should increase, since the current multi-stakeholder model of internet governance is under pressure from several states. Differences over governance are growing and diplomats should play a central role in settling this dispute in international fora.

Diplomats should also take a note of future trends in cyber developments. The cyber preparedness of states will become a more central theme in business decisions in the future. Strong national cyber capabilities will be an important deterrent to cyber crime actors and the image of providing secure platforms will contribute to a better business environment. The private sector might start looking into national cyber security readiness in investment strategies in the future. States with a weak cyber index will be not attractive. In a way, cyber security could become a part of foreign economic policy to attract capital and talent. Although most resilience measures should be taken by private actors, governments need to guarantee sufficient ability to react to serious systemic cyber threats. Developing international and regional early warning and consultations mechanisms in cyber security are additional long term challenges that governments will face. This cannot be achieved without the involvement of diplomatic communities worldwide.

Currently, there are very few nations where national cyber coordination is efficient and the state is able to speak with one voice in all international fora. Typical challenges that all diplomats are likely to face include the structural problem of weak national policy coordination, institutional 'silofication' of cyber policy, inter-departmental confusion regarding national leadership, powerful domestic agencies overriding foreign policy arguments, and the lack of generalists in domestic cyber policy fields who would be able to translate technical jargon to diplomats. If the state does not have a national cyber

2 There is no comprehensive data available yet available on cyber crime losses and intellectual property theft. Indirect evidence on the magnitude of the issue can be found at several sources, for instance at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf or http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr.

strategy and there is no structural cyber coordination in place, it will be very difficult for the foreign policy community to formulate informed policy options. A necessary process for all nations is to develop a national cyber security strategy and to establish a framework for cyber coordination where major government departments have a role.

Diplomats need to coordinate views regularly with national cyber policy regulators, high tech crime units, lawyers, critical information infrastructure protection agencies, national cyber incident response authorities and intelligence analysts in order to maintain an overview and understanding of this fast developing field. Operational details aside, they need to understand how technology works so that they are able to recognise possibly shallow arguments presented by other states in international fora. They should know about trends in national cyber regulation and cyber threat development globally. Like nuclear-era diplomats, they should understand the effects of destructive cyber tools and how critical infrastructures could be used for paralysing states in future conflicts. It would be ideal if the foreign policy community could be part of national cyber exercises annually and learn how to communicate internationally a large-scale cyber attack on a nation.

As we currently live in a world where cyber policy communities are still maturing and the majority of states have no comprehensive national cyber strategies yet, the foreign policy community might find it difficult to find its feet in this field. However, for the future of an open and unfragmented cyberspace, it is absolutely fundamental that diplomats be more active in this field. The technical community has been driving international developments in this field for too long. The time is ripe now to place both domestic and international cyber policies into the strategic context of international relations, international economic developments and national security. For this we need senior national decision-makers, diplomats, lawyers and other non-technical communities to learn quickly about this new policy field and start participating in global cyber debates.

3. The Current Agenda for International Cyber Relations

3.1 International Security and Building Trust in Cyberspace

Trust and confidence are scarce commodities in cyberspace. Old and new rivalries are being played out between states also in this domain. Most recent international conflicts have included cyber aspects, and we have witnessed an international armed conflict where cyber attacks were coordinated with military advances.

Contrary to the conventional wisdom that cyber warfare only recently emerged from the darkest shadows of the internet, the history of conflict in cyberspace dates back to the 1980s. State development of cyber tools to manipulate ICT systems and retrieve sensitive

government and military secrets has been going on for 25 years.[3] Since the dawn of computer systems, governments have been developing and acquiring sophisticated cyber tools. States with powerful militaries have invested heavily in the protection of information systems guarding national security secrets and the safety of nuclear weapons. Some states have developed significant capabilities using ICT technology for both defensive and offensive purposes. Until recently, these tools have usually been well-contained and used for governmental and military purposes only.

Increasingly, private sector actors have noticed malware in their systems that goes beyond the sophistication level that criminal actors can reach. In other words, we have entered an era of possible cyber-induced disruptions and destruction where civilian critical infrastructure will be a likely target. Sophisticated cyber tools are also used for industrial espionage by some governments, leading to a serious loss of intellectual property for companies. Therefore, a task lies ahead of diplomats as to how to regulate the cyber domain and agree on certain rules regarding how state actors should behave.

Due to the complexity and asymmetry of cyberspace, governments will have difficulty knowing in real-time who is behind cyber attacks. The same cyber attack can be regarded as cyber crime, cyber riot or cyber warfare, depending on its motives. The same incident can affect many different domestic cyber communities simultaneously, and anonymous intruders are hard to identify in real-time. Therefore, governments have started to build trust and confidence in politico-military cyber relations to avoid possible misinterpretation of cyber incidents and unnecessary escalation. CBMs for cyberspace are discussed currently in OSCE and in the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF).

Some governments have been calling for new universal cyber treaties and conventions to regulate the behaviour of state actors in cyberspace. This approach might be appealing to novices in the cyber policy area who do not understand the complexities of the issue. Unfortunately, due to the vast number of actors and the dual use of ICT technology, a global cyber convention is almost impossible to develop. As ICT technology is civilian in its nature, verification of any cyber arms treaty will be next to impossible to implement, at least with current technology. Even if states agree on non-first use policy, they could always find a proxy actor to carry out such activities. A better idea is to declare cyberspace a global heritage of mankind where no acts of aggression should be carried out and divert more resources into fighting cyber crime. This might be an idealistic idea, but it also presupposes that serious international players do not offer 'safe havens' to cyber criminals in their territories.

The other reason why liberal democracies do not support the development of a cyber treaty or convention is based on the assumption that this will be used as an international

---

3 For solid overview of cyber conflict history, see 'A Fierce Domain: Conflict in Cyberspace, 1986-2012' ed. Jason Healey, *Cyber Conflict Studies Association Publication in Partnership with the Atlantic Council*, 2013.

pretext to give legitimacy to censorship in cyberspace. Instead, the West would insist that IHL apply in cyberspace. Instead of a treaty, a common understanding should be reached on a set of norms that will assist to de-escalate cyber conflicts in the future.

The NATO Cooperative Cyber Defence Center of Excellence convened an independent group of international lawyers in 2009 to analyse how IHL applies in cyberspace. The effort of a group of 30 leading international law experts, led by the United States (US) lawyer Michael Schmitt, was published in 2013.[4] The manual represents a useful first step for further legal analysis of rules applying to possible warfare in cyberspace. Very importantly, it serves the political purpose of diminishing the pressure to develop a universal cyber warfare treaty.

The development of CBMs as a first set of cyber norms emerged from the OSCE cyber discussions. Possibly the watershed event in contemporary cyber diplomacy took place on 17 March 2009 in Vienna. It was a Cyber Security Workshop following an Estonian initiative during its chairmanship at the OSCE Forum for Security Cooperation in 2008.[5] The workshop indicated the early beginnings of cyber diplomacy where the heads of national cyber agencies participated in the OSCE workshop and tried to understand what they could do in this room full of diplomats. Since then, an international cyber diplomacy agenda has started to develop. OSCE held several other high-level cyber security meetings in 2009-2010. Central themes of discussions included cyber security awareness, determining responsible state behaviour in cyberspace, and the need of national capacities to fight cyber threats. After 2009, when President Obama's administration announced the new US international cyber policy, the US government started to lead the OSCE cyber agenda. The Joint Meeting of the OSCE Forum for Security Cooperation and the OSCE Permanent Council held in June 2010 was a useful event in paving the way for the strategic cyber security discussions. The US proposed at this meeting to discuss norms for state behaviour. At a similar meeting in 2011, the US proposed to start working on CBMs for cyber security. The parallel process of completion of the 2010 UN GGE report also showed that there is enough consensus over CBMs in cyberspace. In April 2012, an informal OSCE Working Group, chaired by the US, was created under the auspices of the Security Committee. The process in the OSCE is still going on and has attracted many other governments to support the norms-based approach. OSCE is the first organisation discussing cyber norms in a wider, multilateral framework. The possible next step would be to take up the issue at the ARF format, where China also has a seat.

In parallel with OSCE discussions, Russia and the US have agreed on an initial set of cyber CBMs, such as crisis hotlines and other measures, through a series of bilateral

4 See *supra* note 1.

5 See OSCE Press Release, *OSCE can play important role in cyber security, says Estonian Defence Minister*, 4 June 2008, http://www.osce.org/fsc/49775.

meetings.[6] Similar bilateral agreements might be under discussion between other nations.

Around the same time as the OSCE development, international cyber discussions started at the UN. In the UN framework, security-related cyber discussions have taken place within the Disarmament Committee. In 2009, the UN resolution 64/386, 'Developments in the field of information and telecommunications in the context of international security',[7] was adopted. The resolution called on states to continue discussions about cyber security, and established an informal GGE that would issue further recommendations. In 2010, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[8] prepared a report that called on states to enhance international cooperation and intensify dialogue among states to reduce cyber risks. The report points out that states are developing tools for cyber warfare, and individuals and criminal organisations are likely to act as proxies and use these tools. It calls for reducing the global risks, to continue further dialogue, and to support capacity building in less developed states. The 2010 UN GGE report on cyber security stated the consensus that IHL applies in cyberspace. Once cyber attacks reach the threshold of an armed attack, states should conduct their activities according to the rules of warfare. These include several principles, as the distinction between military and civilian targets, proportionality, etc. The question of when a cyber attack actually reaches the threshold of an armed attack is far more difficult to determine. The 2010 report confirmed that Article 51 of the *Charter of the United Nations* (UN Charter) on self-defence applies if cyber attacks are causing similar consequences to a conventional armed attack. A new round of discussions of the UN GGE started in August 2012. A new UN GGE report prepared in 2013 continues to stress the need for confidence building and cooperation measures to increase trust in cyberspace. It also confirms the applicability of international law, specifically the UN Charter. It recognises capacity building efforts and tasks states with taking responsibility for the internationally wrongful acts emanating from their territory. In general, it is a good continuation of the norms building process in cyberspace.

3.2 International Initiatives in Fighting Cyber Crime

Due to the complexity of cyber criminal offences and the involvement of multiple jurisdictions in most cyber incidents, it is extremely difficult for law enforcement and other governmental authorities to address this new threat without extensive international cooperation. Transnational cyber crime offences are difficult to investigate and

6 'U.S. and Russia sign pact to create communication link on cyber security', *Washington Post,* 17 June 2013.

7 UNGA, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/64/386, 2 July 2009.

8 UNGA, Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/94, 24 June 2010.

prosecute. Many states in the world are not able to address cyber crime in their territory, and could become 'safe havens' for cyber criminals or cyber proxy actors.

In recent years, cyber criminal networks have grown and merged with serious organised crime groups. International organised cyber crime networks have become ever more powerful, increasing the vulnerability of advanced industrial economies, as well as of emerging states. Cyber crime networks could be also used by hostile states or terrorist groups. Therefore, fighting cyber crime should be at the centre of any cyber foreign policy efforts in order to help the law enforcement authorities to cope with this growing threat. A successful cyber crime investigation requires broad international judiciary and law enforcement cooperation. In some regions, a weak law enforcement capacity to deal with cyber criminal organisations poses a global challenge. It is difficult to reach out to the regions where high tech crime units and legal frameworks to prosecute cyber crime are missing.

There are already significant efforts undertaken by several international organisations, private sector and law enforcement actors to take systematic measures for countering cyber crime globally. The CoE has reached approximately 120 states in promoting the CoE *Convention on Cybercrime*, offering criminal justice capacity building and training of judiciary and law enforcement personnel. Many other international organisations and industrialised states have engaged in law enforcement training in developing states.

Possibly the most effective international instrument for contributing to cyber security is the aforementioned *Convention on Cybercrime* (or 'Budapest Convention') which was opened to signatories in 2001. The Convention provides useful guidance regarding minimum national legal frameworks and the basic requirements for international cooperation. Currently, the Convention has 51 signatory states, of which 40 have also ratified the Convention. Many states outside Europe have followed the guidelines of the Convention. The political importance of the Convention lies in the fact that it is the only binding international agreement on cyber issues. States acceding to the Convention are ready to harmonise internal laws and to take the fight against cyber crime seriously. The CoE, together with the private sector and member states, has launched a Global Project on Cybercrime to promote the Convention worldwide.[9]

Many states outside Europe, in Asia and Latin America, have drawn on the Convention's example and have implemented legislative reforms. The increasing number of states joining this Convention provides a significant deterrent to criminal groups. In addition to promoting the Convention, the CoE has been training law enforcement and judicial authorities, and issued guidelines for national cyber security. Annual 'Octopus Conferences' on cooperation against cyber crime have been launched with a large number of key international participants.

---

9 Council of Europe, Cybercrime website, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.

Within the global project, several useful regional and national programmes are funded. A joint European Union (EU) and CoE project on addressing cyber crime in EU pre-accession states in 2010–2013 focused on cyber crime policies and strategies. It also contributed to harmonisation of legislation, law enforcement training, and law enforcement and internet service providers' cooperation. In April 2011, a joint EU and CoE Eastern Partnership regional project on cyber crime was launched. It provided advice on cyber crime legislation, judicial and law enforcement training, financial investigations, and international cooperation.[10] A new EU and CoE cofounded project to address cyber crime, which has a global reach, started in 2013.

The EU adopted a Directive on Attacks on Information Systems in 2013. It seeks to harmonise criminal law across the EU. The directive facilitates law enforcement and judicial authorities' efforts within the Union to take action against this form of crime.[11] It addresses disparities in member states in criminal law and the need for effective police cooperation within the Union. In addition to significantly improved cyber crime legislation, the EU has also a well-functioning network of national cyber crime units. The heads of national units meet regularly under the formal heading of the EU High Tech Crime Units Taskforce. The Taskforce works closely with the Europol and Interpol high tech crime departments, and links up with its US and other international counterparts. In order to aid cyber crime investigation and information exchange between member states, the EU Cybercrime Centre was established in 2013 at Europol.[12] The Centre aims at aiding joint investigations, supports global capacity building in law enforcement training, and brings together law enforcement authorities for other activities.

The G-8 24/7 network for cyber crime maintains a useful list of contact points within the law enforcement authorities. It aids rapid operational cooperation in investigating and prosecuting high tech crimes.

The United Nations Office on Drugs and Crime (UNODC) has been also discussing cyber crime issues for several years, notably through an Intergovernmental Expert Group meeting that was tasked to produce a comprehensive study on the problem of cyber crime. In UNODC, some states have been calling for a new international legal instrument on cyber crime. Given the complexities of entering into discussions about a new global instrument, the time and additional effort it will take, it would be wiser to expand the influence of the already existing Budapest Convention to a global level.

---

10 Ibid.

11 Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *Official Journal of the European Union* 14 August 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

12 Communication from the Commission to the European Parliament, the Council 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', COM (2012) 140 final, Brussels, 28 March 2012.

3.3 Capacity Building in Cyber Security and Addressing Cyber Crime

Capacity building in cyber security is one of the policy areas that has been articulated as a priority for achieving a more reliable global cyberspace. At the Seoul Conference for Cyberspace in 2013, one of the major topics and conclusions was to call all states to get involved in cyber security capacity building. It seems to be one of the most uncontroversial global cyber topics, but its international agenda is still in a formative phase. A couple of meetings took place during the run-up period to the Seoul Conference. Still, there is no coherent overview on what has been achieved, by whom and where. There is also a lack of conceptual clarity about what we mean by cyber capacity building.

It is hardly news that not all states have equal technical capabilities, preparedness or legal frameworks to address cyber threats. Many policy-makers nowadays are looking for models of how to structure the capacity building efforts, what methods to use, and how to measure the efficiency of these efforts. There are a few key issues in capacity building that should be brought to the attention of policy-makers.

First, capacity building in national cyber security should be coupled with efforts to build safer and more reliable connections and communication networks worldwide. The aim should be to add to the security elements already in the package while extending the communication networks into new markets, choosing IT architecture and developing software. As this aim requires more attention to security features by the major private sector players, a public-private partnership can help to build a more reliable and secure global cyber infrastructure. Many developing states have very limited capacity to monitor and manage incidents in cyberspace. To build this capacity, they need to introduce technological and organisational measures for better incident management. Such minimum requirements are needed for setting up the national Computer Emergency Response Teams (CERTs), including specialised training, acquiring equipment and exchange of best practices within the international professional CERT networks.

The second important element is that nations should develop a model where law enforcement agencies link up with CERTs, internet service providers and public-private partnership networks for incident management. The key issue is to invest in training and education, including a broad base of e-skills of the public, computer security knowledge among law enforcement, IT professionals and other relevant national stakeholders.

The third, equally important, element is to have a proper legal framework in place for facilitating investigation and timely prosecution of cyber offences. Ideally, efforts to fight cyber crime should be seen as a part of a broader national strategy in cyber security, which should bring together different stakeholders and facilitate cooperation between different national agencies. Nations need a policy for addressing cyber crime that will create a comprehensive national approach, and help to engage important decision-makers. This includes measures to criminalise offences related to computer crime, and harmonise the minimum penalties with general international practice. It

will be also important to guarantee that procedural law tools for efficient investigations exist. It would be ideal to follow a model of the *Convention on Cybercrime* to make sure that necessary safeguards and conditions exist for the investigation process.

At an operational level it will be crucial to have an adequate overview of the situation to understand the threats, trends and patterns of cyber crime. It would be equally important to establish a reporting mechanism of cyber crime incidents for individuals and for public and private sector organisations. Additionally, in order to assist law enforcement investigations, police forces need to have special cyber crime or high tech crime units with dedicated computer crime experts. The police should master a certain level of knowledge as to how to collect evidence, and should be supported by computer forensic experts. The operational police units should be supported by similar units within judiciary authorities for efficient prosecution.[13] Finally, effective cyber security capacity building needs a functioning national CERT, which will be the centre of the coordination efforts in a state, which feeds information to law enforcement and acts as an interface between government agencies and the private sector. CERT, private sector and information security networks in a state need to be brought together for a longterm sustainable incident response and monitoring system.

Cyber security activities need to take into account the networked nature of this domain, and include all stakeholders. The number of stakeholders in cyber security is high and capacity building approaches must be coherent across borders and consistent over time. Attention should be focused on prevention and it is crucial to invest in cross-border prevention strategies. Successful capacity building will promote a community building approach and cooperation frameworks. Capacity building will be sustainable if there is a public-private partnership, a minimum national organisational and technological capacity in incident response, and relevant institutional frameworks. The grassroots approach that harnesses local involvement and expertise has proven to be the most desirable approach to capacity building, but sometimes the clear commitment of national governments is required to guarantee high level political buy-in.

Only if all these national building blocks exist will successful international and regional cooperation be possible in each field of cyber security: law enforcement, critical infrastructure protection, CERT networks and national security communities. Better cyber security will always be a result of coordination and cooperation among a wide range of players.

Tensions around internet freedom and freedom of expression online might conflict sometimes with a genuine wish of states to gain better cyber security capacities. Capacity building assistance should not be used for unjustified government control and mass

13 See Heli Tiirmaa-Klaar, Jan Gassen, Elmar Gerhards-Padilla, and Peter Martini 'Botnets' *Springer Briefs in Cybersecurity* (Springer 2013).

censorship. Current differences between governments over the freedom of expression will likely remain, and can hinder the development in capacity building. However, there is always a common denominator that concerns different political regimes: how to guarantee an online environment for their citizens which is free of fraud and crime.

Currently, international cyber security capacity building activities are numerous, but still sporadic. Better stocktaking and overview is necessary to steer efforts globally. There is also a need for analysis of regional and functional focus for capacity building, and for international coordination mechanisms. For a successful capacity building model, best practices from development cooperation experience and cyber security should be integrated. It will be also important to set up a clearinghouse mechanism between donors and recipients.

Finally, existing, informal, international cyber resilience cooperation networks will be valuable for cyber security capacity building.

A few informal international forums exist in the cyber security field which provide for policy development and exchange of best practice. The Meridian process maintains the regularly updated global reference book for critical information infrastructure protection policies, with points of contacts for technical cyber authorities in more than 50 states. As this forum is limited to governmental representatives only, it connects national cyber security policy-makers and technical experts. Meridian has annual and regional events, and serves as a major professional cyber forum that builds global trust and facilitates consultations between policy-makers. The Meridian network also issues recommendations, shares best practices, offers IT security guidelines, exercise manuals and other information to its participants.

The Forum of Incident Response and Security Teams (FIRST) network connects CERTs all over the world, and serves as a forum for the technical community. Within FIRST, IT security experts exchange information and experiences in incident response practices. FIRST is largely built on the trusted network of personal contacts, and it has served already as a useful platform from which to react in times of cyber crises. There are plenty of information security expert forums, which serve the same purposes, and have been, so far, the major mechanisms in connecting the professionals, whose everyday work is to guarantee the stability of the global ICT sector. In the absence of institutional crises management mechanisms, these informal networks have saved the internet many times. FIRST also accredits CERTs worldwide.

3.4 Defending Human Rights in Cyberspace

Different visions of cyberspace governance are also played out in the traditional foreign policy field of the protection of fundamental rights. The advent of the internet has made it easier to communicate between different social and political groups in non-democratic regimes, but these regimes have quickly learned how to use ICT technology

to stay in power. Concerns are growing over the use of ICT technology for censorship, curtailing freedom of expression online and using social media for neutralising political opposition. Human rights debates include increasing concerns over internet freedom, the boom in internet surveillance technologies, and freedom of expression in electronic media. With many governments ordering new technologies to maintain control over an ever active blogosphere and social media, human rights debates online also include issues such as corporate social responsibility, trade restrictions and sanctions.

Diplomats pursuing cyber security dialogues should be aware of fundamental freedoms restrictions online. In many instances, and due to the legacy of this technology-driven subject, cyber relations between states might be still carried out by technical level agencies or domestic line ministries, where internet freedom is often not a central concern. In order to mainstream cyber relations into overall political engagement with foreign partners, and ensure that the security and freedom aspects will be balanced, ministries of foreign affairs should assume a coordinating role in external cyber relations.

On 5 July 2012, the United Nations Human Rights Council passed a resolution on 'The promotion, protection and enjoyment of human rights on the internet'.[14] The landmark resolution stresses the Universal Declaration of Human Rights, the *International Covenant on Civil and Political Rights* and the *International Covenant on Economic, Social and Cultural Rights* and the importance of exercising human rights during the rapid pace of technological development. The resolution confirms that all individuals are entitled to the same human rights and fundamental freedoms online as they are offline, and all governments must protect those rights regardless of the medium. During the negotiations of the resolution, the US worked closely with the main sponsor, Sweden, and over 80 states acted as co-sponsors, including Brazil, Turkey, Nigeria and Tunisia. The resolution includes an often quoted passage '[...] the same rights that people have offline must be also protected online, in particular freedom of expression [...]'. Freedom of expression online is also stressed in the EU Strategic Framework and Action Plan on Human Rights and Democracy, where the Action Item 24 'Freedom of expression online and offline' calls for several measures to protect fundamental rights online.[15] A similar principle is added to the 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' in the EU international cyberspace policy section.[16] Also the G8 confirmed human rights online through the Deauville Declaration on Renewed Commitments for Freedom and Democracy and the Deauville Declaration on

14 UNGA, 'The promotion, protection and enjoyment of human rights on the Internet', UN Doc. A/HRC/20/L.13.

15 EU Strategic Framework and Action Plan on Human Rights and Democracy, adopted by the Council of the European Union, 25 June 2012, 11855/12.

16 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', by European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, Brussels 7 February 2013, JOINT (2013)1, pp.14-16.

the Arab Spring. The human rights agenda in cyberspace is a separate and not very well understood field outside of the human rights community, since it includes a wide range of topics and instruments of foreign policy.

An influential instrument is to support Corporate Social Responsibility (CSR) in using the dual use technologies. Several actions at a global level have contributed to this objective. The UN Human Rights Council endorsed a set of UN Guiding Principles on Business and Human Rights in 2011. The Principles establish a global standard for the role of businesses and governments to ensure that companies will respect human rights in their operations and through their business relationships. The European Commission Communication, 'A renewed EU strategy 2011-2014 for Corporate Social Responsibility' aims to enhance the visibility of CSR policies and disseminate good practices. It calls to improve the level of trust in the EU's private sector, improve self- and co-regulation processes, and better align EU activities with the global approach to CSR. To follow the UN Principles, the European Commission developed guidance on corporate responsibility in respecting human rights in the ICT sector.

The second instrument available for diplomats is to set regimes for export control, brokering and transit of dual use items. The objective is to limit the widespread sales of technologies that might be used for internet surveillance. Although this policy option is available, it is quite difficult to have an indisputable assessment of the risks relating to the delivery of dual technologies to a given state. Some of these technologies are used in counter-terrorism activities and other legitimate fields.

The third policy option is to use sanctions to prevent authoritarian regimes from using technologies that are harmful for human right defenders. Such sanctions have been imposed by the EU on Syria and Iran in relation to equipment or software intended for the interception of communications. The measures were first introduced in 2012 on sale, supply, transfer or export of equipment or software intended for use in the monitoring of or interception by the Syrian regime. In a Regulation of 18 January 2012, the scope of the measures was clarified. The Regulation determines precisely to which equipment, technology or software the export ban applies. The Regulation also prohibits the provision of technical assistance, brokering services, financing or financial assistance, or the provision of any telecommunications or internet monitoring or interception services.[17] A similar regulation was published on Iran in 2012.[18]

Defending human rights in an era of technology is a challenge and, therefore, liberal democracies should certainly safeguard the principle of fundamental rights in

[17] Council Decision 2012/36/CFSP of 23 January 2012 amending Decision 2010/639/CFSP concerning restrictive measures against Belarus, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:019:0031:0032:EN:PDF.

[18] Council of the European Union Decision 2012/168/CFSP amending Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in Iran', 23 March 2012, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:087:0085:0089:EN:PDF.

technology transfer and export. The same like-minded group of governments should also continue the endeavours to keep the internet open and unfragmented, free of direct control by governments.

3.5 Controversy over Internet Governance

As with other ICT technologies, the internet has been developed and maintained by private sector actors. Its governance layer has been added to technical layers in a non-profit format, under the guidance of the Internet Corporation for Assigned Names and Numbers (ICANN). This organisation has a coordinating or regulating function of the internet policies. ICANN deals with the internet's systems of unique identifiers, DNS, and other policy issues. Governments have a seat in ICANN's Government Advisory Committee (GAC), which is one of the governance bodies advising the ICANN Board.[19] The internet governance world is still run by technical communities mostly, since the routine issues and decisions require a technology background.

The decision to create ICANN in the 1990s was a reaction to the International Telecommunication Union's (ITU) claim to be the principal organisation over internet governance functions. Ever since, the ITU has sought new ways of taking over the internet governance role. Liberal democracies have a justified concern that the inter-governmental model of internet governance will lead to one that is fragmented, slow and not interoperable. National oversight will also facilitate censorship online in authoritarian states.

Currently, the Internet Governance Forum (IGF) and the World Summit of the Information Society (WSIS) are the major global discussion fora on this issue. The IGF takes place annually and brings together the global stakeholder community, where governments, the private sector and the civil society discuss internet-related topics. UN discussions on internet governance have crystallised around two major categories. First, there is a group of states supporting ICANN and proposing more effective multi-stakeholder governance, including closer government involvement in ICANN decision-making. Second, there is another group of states less supportive of ICANN, and looking for an alternative inter-governmental governance structure for the internet. This group of states would like to challenge the existing model of internet governance, and calls for 'enhanced cooperation', which means more government control in this context.

During the World Conference on International Telecommunications (WCIT) in Dubai in 2012, 93 governments supported an enhanced role of the ITU over internet regulation. While the EU Member states, the US and other like-minded states did not sign a new ITU treaty at WCIT, the vote on this issue showed a widening global polarisation over internet governance. The US and EU advocate the existing model of internet oversight

[19] ICANN website, https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee.

by multi-stakeholder, non-governmental institutions. Many developing and emerging states support transfer of regulatory power of the internet to the ITU.

A couple of emerging powers convene regularly to discuss internet governance, content management, and cyber security issues. They see their special role in promoting the interests of developing nations, and propose that the internet must be managed by governments, with a particular focus on the influence of social networks on society.

Some developing states, which are not able to deal with cyber threats, blame the faults in internet security on the owners of its basic infrastructure and the ICANN-led governance structure. For many, less open states, a new, government-controlled model is attractive as it would allow them to implement censorship more easily. Therefore, they have joined emerging nations to challenge the current model. However, what is not really explained well internationally is that an inter-governmental model of internet governance might lead to a lack of fundamental rights protection, the fragmentation of an interoperable internet and negative economic consequences. More awareness is needed to support the arguments for a free and open internet, which will be the primary role for cyber diplomacy. It will be also necessary to offer development assistance to states that cannot cope with cyber security threats.

The international community should certainly avoid another WCIT experience, where polarisation on this issue took place. The next WSIS in 2015 should be well prepared and coordinated, with the involvement of the cyber foreign policy community. The time has come to turn around the trend where internet governance was viewed only as a 'geek subject'. In order to preserve the multi-stakeholder model, ICANN should also become more accountable to legitimate public policy interests, such as law enforcement concerns.

For diplomats, it will not be easy to learn to orient themselves in this sub-field of cyber diplomacy. Debates on the internet take place at a myriad of different fora, events, conferences, symposiums and stakeholder meetings. Due to the large number of meetings, some of which are very technical, even an experienced cyber observer will get confused. Indeed, the complexity of the issue is magnified by the overlap of work-streams and many separate communities dealing with the whole spectrum of internet governance.

4. Mission for Cyber Diplomacy in the Future

The agenda for cyber diplomacy is a vast one. Among all the different subjects, five areas described above – human rights, international security, internet governance, cyber crime and capacity building – should be priorities for diplomats. There are plenty of other areas where diplomats must orient themselves, such as trade in ICT products, technology transfer, national cyber regulations, cyber defence and many other issues. It will be impossible to be an expert in all these areas at the same time. Therefore, the best

results of cyber diplomacy are achieved if the foreign policy community works in close cooperation with national policy-makers, the private sector and academia.

There are some challenges that diplomats will meet in their future efforts to steer international cyber relations. The first is to concentrate on structural issues and prioritise forward-looking processes in the above-mentioned five areas. It will be easy to get distracted by the volume of currently ongoing, less relevant cyber activities. This chapter lists only a small fraction of international cyber initiatives, but there are many more out there, either government or private sector led. The myriad of events, conferences and initiatives is likely to grow in coming years as many businesses and special lobby groups try to establish their cyber programmes. Although the current tendency for too many cyber gatherings with no clear deliverables will certainly raise awareness, fragmentation of efforts is not desirable.

The second objective for diplomats should be to raise the knowledge basis in MFAs in all cyber issues, and to keep their geographical colleagues on track of the most recent developments. Internal cyber coordination structures in foreign ministries are easy to set up and do not require additional resources, but will greatly contribute to the mainstreaming of cyber issues into external relations.

The third mission is related to institutional issues and to inter-departmental coordination. It will be indispensable to have a coherent voice on strategic international cyber issues if a state wants to be a global player. The challenge might be that a small foreign policy community needs to constantly educate a vast domestic cyber policy community on international cyber issues. It is a difficult task in the long run. Therefore, a National Cyber Security Council or a similar senior level government body is needed to make sure that international cyber policy concerns are heard among all ministries.

The fourth challenge is to insert a little more idealism into the current over-securitised cyber agenda. As cyber developments are often dominated by strong national security agencies, military industry lobby groups and the like, we might end up in a dangerous vicious circle. Security agencies would always report that other states' agencies are ahead in capability development, and so all governments are bound to follow the spiralling effect of militarising cyberspace with destructive capabilities. The role of diplomats is to come to an agreement on a cyber norms process, and to work towards a more peaceful future in this domain.

The fifth mission for cyber diplomats is to encourage the political science and international security academic community to build conceptual and analytical work on cyber issues. Most academic efforts now are still taking place in the technical area, and not too many social scientists have entered the field of cyber security research. Therefore, a very limited number of solid academic contributions exist that could assist national policy-makers in offering basic analytical frameworks for cyber policies.

'Cyberspace studies' could become a sub-set of Security Studies, International Relations, International Economic Policy and Trade, or other academic fields. These studies could include fascinating topics like how power relations between states have changed in the cyber era, how IT security demand has contributed to privatisation of national security and how the protectionist policies in IT security are damaging the multilateral world order that governments have been building up for the last 60 years. Key concepts from International Relations and Political Science literature could be effectively used in further development of theoretical cyber studies area in International Relations.

Illustrating the early stage we are still at with cyber diplomacy, there is only one international initiative that tries to bring all these different streams of work together. It is a global Cyberspace Conference that started in London in 2011, continued in Budapest in 2012 and in Seoul in 2013. This conference is a primary forum for experienced and new cyber diplomats. The conference is the place to articulate global stakeholders' views on cyber issues. It is also the first global initiative that has been able to bring diplomats on board and complement other cyber gatherings fragmented between different thematic communities. Hopefully, the conference will continue to attract the attention of major world players, as well as help diplomats to keep this complex issue on the agenda of high level political decision-makers.

Katharina Ziolkowski

Confidence Building Measures for Cyberspace

1. Introduction

The present chapter* describes the nature of confidence building measures (CBMs) and illustrates the current developments within the international community which aim to elaborate such measures for cyberspace. For the purposes of the present analysis, cyberspace is understood as a global, non-physical, conceptual space, which includes physical and technical components, i.e., the internet, the 'global public memory' contained on publicly accessible websites, as well as all entities and individuals connected to the internet. Cyberspace has political, economic, social and cultural aspects going far beyond the notion of a pure means of information transfer.

CBMs are a verified instrument of international politics, which aims to prevent the outbreak of (declared) war or of any other armed conflict between States (hereinafter referred to as 'international armed conflict') by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis situation. CBMs achieve this by establishing practical measures and processes for (preventive) crisis management between States. Due to the specific features of the internet, the development of CBMs for cyberspace proves to be difficult. As indicated by current discussions, CBMs for cyberspace will display the nature of political commitments. Political declarations of States are a powerful tool of international relations. Importantly, they are significant for the progressive development of international law.

However, before presenting the above-mentioned aspects in more detail, it is of the utmost importance to acknowledge the politico-historic context of CBMs for cyberspace (2). It not only mirrors the dynamics within the international community with regard to international peace and security in the cyber realm, but also influences the current developments concerning CBMs. Thereafter, the concept and cyber-specific aspects of CBMs will be presented (3). Furthermore, the relationship between political and legal commitments will be examined, focusing on the importance of political declarations for the interpretation and development of public international law (4). These sections will be followed by some concluding remarks (5).

* The present chapter contains information on the development of confidence building measures for cyberspace as of 15 August 2013. Due to limited research resources, the assessment of secondary legal sources is primarily based on scholarly writings available online. The author is deeply indebted to the NATO ACT – SEE Legal Office for providing access to various online databases.

2. Politico-Historic Context

The end of the Cold War coincided with several strategic decisions of the United States (US) government, and with technical developments, which laid the foundations for the transformation of the academic research networks, which were mainly geographically based in the US, into the internet as it is known today.[1] Two decades later, the internet is deemed a truly global network, indispensable to political, economic, social and cultural life in post-industrial States. At the same time, a revival of Cold War metaphors in the context of cyberspace is perceivable in the media and in political and legal science.[2] Indeed, the perception of cyber security, formerly viewed as an exclusively technical and organisational challenge, has undergone a strategic shift. Cyber security has become an inherent part of national security, as evident by the multitude of national cyber security strategies issued[3] since 2008, and thus also a matter of international peace and security.

Some States emphasise the potentially deadly characteristics of cyber tools and the risk of cyberspace transforming into a new global battlefield.[4] Indeed, the armed forces of several States tend to consider cyberspace the fifth domain of warfare (beside land, sea,

---

1 The US decommissioned the Advanced Research Projects Agency Network (ARPANET), initially developed by the US Department of Defence for collaboration in the context of scientific defence research projects (28 February 1990), and disconnected the US Computer Science Network (CSNET) (October 1991). The US agency National Science Foundation (NSF) opened the succeeding main network (NSFNET), which subsequently built the backbone of the internet, for other than academic or educational purposes (March 1991). The introduction of the first World Wide Web service of hyperlinked documents, ie, websites, by a CERN scientist shaped the current feature of the net (6 August 1991). See Johann-Christoph Woltag, 'Internet' in Rüdiger Wolfrum (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press 2008, online edition [www.mpepil.com]) [in following MPEPIL] MN 2; National Science Foundation, 'A Brief History of NSF and the Internet' (Factsheet, 13 August 2003) <http://www.nsf.gov/news/news_summ.jsp?cntn_id=103050>; Vincent Cerf, 'How the Internet Came to Be' (1993) <http://www.virtualschool.edu/mon/Internet/CerfHowInternetCame2B.html>; CERN, 'The birth of the web' <http://home.web.cern.ch/about/birth-web>.

2 eg Noah Schachtman and Peter W Singer, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive' (Brookings Institution Paper, 15 August 2011) <http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx>; David Singer, 'In cyberspace, New Cold War' *The New York Times* (24 February 2013) <http:// www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?pagewanted=all>; Yasmin Tadjdeh, 'U.S. Engaged in "Cyber Cold War" with China, Iran' *National Defence Magazine* (7 March 2013) <http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1075>. For scientific contributions see eg Matthew Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale Journal of International Law 421, 425ff; Brandon Valeriano, 'Mind the Gap? Deterrence in Cyberspace' *New Atlanticist* (11 July 2012) <http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace>.

3 See selection of publicly available strategic cyber security documents at NATO CCD COE, National Strategies & Policies website <http://ccdcoe.org/328.html>.

4 eg the Chinese statement at the United Nations General Assembly, noting that the 'international community […] must work to prevent the information space from becoming a "new battlefield"', UN Doc A/DIS/3467 (1 November 2012); Sergey Fedosov, 'Statement by the Russian participant at the UNIDIR Cyber Security Conference (Conference 'What does a Stable Cyber Environment Look Like?', UNIDIR, Geneva, 8-9 November 2012) <http://www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf>; Noah Schachtman, 'Darpa Looks to Make Cyberwar Routine With Secret "Plan X"' *Wired* (21 August 2012) <http://www.wired.com/dangerroom/2012/08/plan-x/>.

air and space).[5] A United Nations Institute for Disarmament Research study of 2011, based on a review of open-source documents, 'identified 33 States [out of 133 States] that include cyber-warfare in their military planning and organisation'.[6] Despite severe deficiencies[7] in the study, it is undeniable that several States have, or are thought to have, such capabilities at their disposal, or are developing them. However, only very few[8] have issued publicly available cyber security or defence strategies for the military sector, and only one[9] directly addresses offensive cyber activities. In general, States rather emphasise the dependency of the armed forces on the availability and integrity of information and communication systems (ICTs) as well as on the confidentiality of data, and thus the aspect of cyber security or defence. Yet, according to a European Defence Agency study of 2013, many States remain at an early level of maturity with regard to the doctrinal and organisational development of their cyber defence (or security) frameworks.[10]

To a certain extent, the 'cyber war' discussion is driven by an overestimation of the scope and consequences of malicious cyber activities, and by an underestimation of the technical expertise and operational sophistication required to launch a 'cyber attack'. The questions of complexity and accessibility of potential target computer systems, e.g., networks supporting critical infrastructure systems, are widely disregarded.[11] As

5 eg United States of America, *Department of Defense Strategy for Operating in Cyberspace* (July 2011) 5; The Netherlands, Ministry of Defence, *The Cyber Defence Strategy* (June 2012) 4; Japan, Ministry of Defence, *Toward Stable and Effective Use of Cyberspace* (September 2012) 3.

6 James A Lewis and Katrina Timlin, 'Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization' (UNIDIR Publication, October 2011) 3 <http://unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf>.

7 A closer look at the study reveals that States building up, or having at their disposal, cyber security capabilities, eg, Albania, are considered as States 'including cyberwarfare in military planning and organisation', although, eg, Albania is in the course of establishing a national Computer Emergency Response Team (CERT) with the support of the Carnegie Mellon University, Software Engineering Institute (SEI), and the USAID (development aid agency of the US State Department); see 'SEI grounds Albania-USAID Effort in CERT', Carnegie Mellon University, Software Engineering Institute website <www.sei.cmu.edu/newsitems/rmm-usaid.cfm>. The above was corrected by James A Lewis, 'Cybersecurity and Cyberwarfare: Assessment of National Doctrine and Organisation' in UNIDIR, *The Cyber Index. International Security Trends and Realities* (UNIDIR Publication 2013/3) 9.

8 These are Russia, the US, the Netherlands and Japan. See Russian Federation, Ministry of Defence, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* (2011, unofficial translation) <http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf> 4ff (see, for example, the definitions of military conflict in information space, information war, information weapons); United States of America (n 5) 5 ('Given its need to ensure the ability to operate effectively in cyberspace and efficiently organize its resources, DoD established U.S. Cyber Command (USCYBERCOM) […]'); The Netherlands (n 5) 11 ('Focal Point 3: Offensive'); Japan (n 5) 4 ('The MOD and SDF [Self Defence Forces] must aim to acquire cutting-edge capabilities in cyberspace just as they do for other domains in order to fulfil its missions such as national defense.').

9 The Netherlands (n 5).

10 RAND, 'Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) prepared for the European Defence Agency' (unclassified summary, March 2013) 7.

11 John B Sheldon, 'Achieving mutual comprehension: why cyberpower matters to both developed and developing countries' in Kerstin Vignard (ed), *Confronting Cyberconflict* (UNIDIR Disarmament Forum Series 2011/4)

most of the current malicious cyber activities are to be categorised as economically or politically motivated cyber crime, including cyber espionage, scholars caution against an inappropriate militarisation of the topic.[12] Conversely, national security and intelligence advisors,[13] by nature, emphasise the dangers emanating from potential malicious cyber activities. Consequently and understandably, many States believe that, even if by misperception and miscalculation of the risk, malicious cyber activities could result in a conventional, or even nuclear,[14] military conflict.[15]

Discussions of an international agreement to limit the risk of 'cyber conflict' have been conducted at the diplomatic level since the 1990s.[16] In 1998, the Russian Federation proposed for the first time an 'arms-control' treaty that would have banned the use of cyberspace for military purposes.[17] In general, the aim of arms control regimes is to reduce the risk of the outbreak of an international armed conflict by reducing the existence or restricting the use of certain weapons.[18] However, for the time being, the

41ff; Tom Gjelten, 'Is All The Talk About Cyberwarfare Just Hype?' *GBP News* (15 March 2013) <http://www.gpb.org/news/2013/03/15/is-all-the-talk-about-cyberwarfare-just-hype>.

12 eg Ryan Singel, 'White House Cyber Czar: "There is No Cyberwar"' *Wired Magazine* (4 March 2010) <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>; Myriam Dunn Cavelty, 'The Militarisation of Cyber-space: Why Less May Be Better' in Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012) 141-153; Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17 Journal of Conflict and Security Law (2) 187, 195-198; Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35 The Journal of Strategic Studies (1) 5, 5ff.

13 Especially interesting is the comment on two different threat assessments given by the Director NSA (US) / Commander US CYBERCOM and of the Director of National Intelligence (US) to the US Senate Intelligence Committee, see Gjelten (n 11); cf Jack Goldsmith, 'Cybersecurity Treaties: A Sceptical View' (Stanford University, Hoover Institution, Koret-Taube Task Force on National Security and Law, February 2011) 5 <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf> (Goldsmith is a former US Assistant Attorney General and Special Counsel to the US Department of Defense); Nazli Choucri, *Cyberpolitics in International Relations* (MIT Press 2012) 150ff; Philip Lieberman, 'We're losing the battle against state sponsored attacks' *Help Net Security* (8 April 2013) <http://www.net-security.org/article.php?id=1825>.

14 cf The President of the United States of America, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (May 2011) 4; United States of America, Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (August 2012) 42; Mark Mazzetti and David E Sanger, 'Security Leader Says U.S. Would Retaliate Against Cyberattacks' *The New York Times* (12 March 2013) <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all&_r=0>.

15 James A Lewis, 'Confidence-building and international agreement in cybersecurity' in Vignard (n 11) 51ff.

16 ibid 52.

17 John Markoff and Andrew E Kramer, 'U.S. and Russia Differ on a Treaty for Cyberspace' *The New York Times* (27 June 2009) <http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all&_r=0>; Ellen Nakashima, '15 nations agree to start working together to reduce cyberwarfare threat' *Washington Post* (17 July 2010) <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html>; Goldsmith (n 13).

18 cf Louise Arimatsu, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations' in Czosseck, Ottis and Ziolkowski (n 12) 91, 99.

majority of experts see little chance of applying traditional arms control regimes to cyberspace.[19]

Any endeavour to *reduce the existence of malicious software* by normative means would fail, as it is, at present, not practicable and politically feasible to integrate any monitoring and verification mechanism into a treaty. Software is not tangible, is easy to hide, and the mathematical functions or patterns are difficult to recognise as malicious without a thorough and lengthy analysis, and reliable information about the intended use. For example, a code-breaker software could be a dual-use tool, which can be used either for purposes of mending an owned network, or for penetration of a foreign military network. Additionally, it is unlikely that any State would agree to external verification measures requiring scans of all (including classified) governmental computers and diverse data storage devices.[20] Moreover, cyber tools can be produced and employed by non-State actors, in which case, the tools' production would not be subject to any effective regulation.[21] Furthermore, States might not be ready to deprive themselves of the possibilities the cyber tools are offering in terms of a potentially non-lethal, precise means of disruption and interference with, e.g., computer networks of opposing forces during a United Nations (UN) mandated military mission. Finally, the possibilities of acting anonymously within the internet (in the meaning of the technical aspects and physical components of cyberspace) and the challenge of attributing the employment of malicious software would make any legal obligation to reduce its existence futile.

The *restriction of the use* of certain 'cyber weapons' would require a definition of that term which is unfortunately often used in the media and in political[22] and legal science[23] without deliberation. Finding a consensus on a definition of 'cyber weapons' or 'information weapons', focusing either on the means, the aim or the effects of malicious software, must be deemed rather illusory.[24] It should be mentioned that international humanitarian law, as a matter of law and not of political choice, already contains specific limitations on the development and use of certain 'weapons, means or methods

19 This opinion is expressed, for example, by the Federal Republic of Germany, 'Cyber security: confidence and security-building measures (CSBMs)', Federal Foreign Office website <http://www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung_/KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html>.

20 Arimatsu (n 18) 101.

21 Georg Kerschischnig, *Cyberthreats and International Law* (Eleven International Publishing 2012) 297.

22 Rex Hughes is predicting the development of a 'new generation' of 'cyber-weaponry' and cyberspace becoming 'ground zero for the next global arms race', see Rex Hughes, 'A treaty for cyberspace' (2010) 86 International Affairs (2) 523ff.

23 eg Goldsmith (n 13) 5-7. Kerschischnig defines cyber weapons as 'cyberspace-borne tools and techniques that interfere with a system's normal functioning', whereas the tools 'can be summarized under the term "malware", such as viruses, worms, Trojans, rootkits and botnets, and the techniques would include Dos, infiltration, social engineering, probing, sniffing and mapping', cf Kerschischnig (n 21) 31. Unfortunately, the definition would also apply to cyber tools used by a network administrator for mending the own system.

24 Arimatsu (n 18) 97ff.

of warfare', that is, including the 'means' of malicious software or the 'method' of employing it.[25]

However, it should be considered that also nuclear and conventional arms control development was historically accompanied by concerns regarding the effectiveness and the feasibility of verification and existing control measures, which have been proven inaccurate over the past decades. Future technological advances could provide feasible (and politically acceptable) verification and control mechanisms for malicious software, although the aspect of skills and knowledge, which plays a crucial role in the intrusion and manipulation of computer networks, could not possibly be addressed by verification and control measures.

At present, an arms control treaty for cyber means is, for the above reasons, deemed not feasible within the international community, so the idea of an international treaty regulating State behaviour in cyberspace has been suggested. On 12 September 2011, China, the Russian Federation, Tajikistan and Uzbekistan proposed, 'in the form of a potential [UN] General Assembly resolution',[26] an *International Code of Conduct for Information Security.*[27] The draft refers, *inter alia,* to non-proliferation of 'information-weapons', stating the obligation of each State: '[n]ot to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies' (para. b).

Also in September 2011, the Russian Federation introduced, during an international security conference, another proposal for an international agreement.[28] The *Convention on International Information Security (Concept)*[29] is based on the same guiding principles as the above-mentioned code of conduct, but shows a much higher level of detail, comparable to the 2009 *Agreement between the Governments of the Member*

25 For a thorough analysis, cf ibid 99 and 103-107. Humanitarian Law contains limitations on the development and restrictions of the use of cyber 'means' or 'methods'. It obliges States '[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.' (Article 36 of the Additional Protocol I of 1977 to the Geneva Conventions of 1949).

26 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General', UN Doc A/66/359 (14 September 2011).

27 ibid annex.

28 The proposal was presented at the 'Ekaterinburg International Meeting of High-Ranking Officials Responsible for Security Matters', hosted by the Russian National Security Council 21-22 September 2011. The draft convention had been elaborated by Russia's National Security Council, the Foreign Ministry and the Moscow State University. cf 'Russia seeks equal cybersecurity for all' *The Voice of Russia* (23 September 2011) <http://english.ruvr.ru/2011/09/23/56634644.html>.

29 Russian Federation, The Ministry of Foreign Affairs, Convention on International Information Security (Concept), <http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument>.

States of the Shanghai Cooperation Organisation[30] *on Cooperation in the Field of International Information Security.* The draft concept proposes, *inter alia,* 21 'basic principles for the international information security' (Article 5), several measures aimed at maintaining and fostering international cyber security (Articles 6-12), as well as a set of definitions of terms (Article 2).

Although addressing a wide range of cyber threats,[31] neither draft has proved to offer the prospect of forming the basis for negotiations within the international community.[32] Inherent to both proposals is the challenge of finding consensus on the definition of terms such as 'hostile activities' or 'information space'.[33] It should be considered that determining a common cyber terminology, even within a single State, or within international organisations such as NATO, proves to be most difficult. Also, translating definitions into a certain language (e.g., English) does not always reflect the cognitive connotations of wording given within the original tongue. Additionally, and adding complexity to the matter, certain terminology (e.g., 'information security', as used by Member States of the Shanghai Cooperation Organisation and including the human cognitive domain, versus 'cyber security' as used by many Western States) indicates different approaches with regard to the always necessary balance between security and civil liberties.[34] Some States emphasise the fundamental principle of public international law, namely State sovereignty, as well as States' territorial integrity, political independence, and aspects of national security and political stability. On the other hand, other States underline the importance of universal human rights, support the idea of free flow of information, and promote close international cooperation in law enforcement, including information sharing.[35] Finally, a truly comprehensive regulation

30 The Shanghai Cooperation Organisation was founded by The People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan on 15 June 2001.

31 Both proposals address the aspects of acts of aggression, cyber crime, terrorist activities, ICT components' supply chain security, and critical infrastructure protection, cf lit b-e of the Draft *International Code of Conduct for Information Security* (n 26), and Article 4 of the *Convention on International Information Security (Concept)* (n 29).

32 eg William Hague, 'The Rt Hon William Hague MP, London Conference on Cyberspace: Chair's Statement of 2 November 2011', Foreign and Commonwealth Office website <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement> ('Some delegates noted the draft Code of Conduct circulated at the United Nations. There was no appetite at this stage to expend effort on legally-binding international instruments.').

33 Lewis deems the challenge of finding a common terminology in the cyber arena 'unsolvable', see Lewis (n 15) 53.

34 cf a thorough analysis by Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in Karlis Podins, Jan Stinissen and Markus Maybaum (eds), *Proceeding of the 5th International Conference of Cyber Conflict* (NATO CCD COE Publication 2013) 413-429.

35 See detailed discussion in Arimatsu (n 18) 94-97; Lewis (n 15) 55. See also declaration of 32 Western States in UNGA on the importance of universal human rights and free flow of information in cyberspace, *General statement in connection with action on L.30 Developments in the field of information and telecommunications in the context of international security* (6 November 2012) <http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com12/statements/L30_Sweden-joint.pdf>; cf the Swedish approach to the internet as a facilitator of justice, equality and human rights, Government Offices of Sweden, *Enhancing*

of State behaviour in cyberspace would need to include also social and economic aspects, making such an endeavour even more difficult, when considering the political and ideological differences within the international community.

Despite all discrepancies, a common understanding of cyber threats as a global challenge to international peace and security led[36] the international community of States to focus the diplomatic endeavours on a rather practical and (relatively) timely remedy, which does not involve the above-mentioned, highly controversial questions, namely the development of politically binding CBMs for cyberspace.

3. Confidence Building Measures for Cyberspace

CBMs, also known in their advanced forms of 'transparency and confidence building measures' or 'confidence-, transparency- and security-building measures', are an instrument of international politics, negotiated by and applied between States. CBMs aim to prevent the outbreak of an international armed conflict by miscalculation or misperception of the risk and by the consequent inappropriate escalation of a crisis situation, by establishing practical measures and processes of (preventive) crisis management between States.[37] In general terms, these measures usually contain aspects of transparency, cooperation, and stability:

- Transparency measures aim to foster a better mutual understanding of national military capabilities and activities. As part of this, crisis management instruments, such as effective crisis communication channels, are usually created and tested; military manoeuvres and movements are notified via diplomatic channels.
- Cooperation measures include exchange of documents (e.g., military doctrines), joint military exercises, exchange of observers, visits of military delegations, and development of common understanding of key terms and definitions.
- Stability measures aim to foster predictability of military activities by limitation of them, and through the stabilisation of the military balance.

The notion of CBMs was developed during the Cold War in order to avoid the deployment of nuclear weapons by accident, and has now widened into other areas.[38] Although certain features recur within the international and regional CBMs developed in the context of specific areas (e.g., outer space) or weaponry, the application of this traditional and established instrument to cyberspace constitutes a complex endeavour.

Internet freedom and human rights through responsible business practices, Sweden, Ministry of Foreign Affairs (13 April 2012) <http://www.government.se/content/1/c6/19/05/60/591bf7d9.pdf>.

36 According to Lewis, alternatives to a formal cyber treaty began to appear already as early as 2008 (aiming at development of politically binding norms for responsible State behaviour in cyberspace), cf Lewis (n 15) 53.

37 cf Zdzislaw Lachowski, 'Confidence-Building Measures' in MPEPIL (n 1) MN 1.

38 cf United Nations Office for Disarmament Affairs, 'Confidence Building', website <http://www.un.org/disarmament/convarms/infoCBM/>.

3.1 Goals, Objectives, Tasks and the End-State Desired

The general goals, objectives and tasks of CBMs are described in the preambles of several CBM documents (e.g., the *Final Act of the Helsinki Conference on Security and Co-operation in Europe*[39] of 1975, Part 2). A condensed formulation can be found in the *Guidelines for appropriate types of confidence-building measures and for the implementation of such measures on a global or regional level*, prepared by the United Nations (UN) Disarmament Commission's Consultation Group in 1988.[40] According to these guidelines:[41]

- '[t]he **ultimate goal** of confidence-building measures is to strengthen international peace and security and to contribute to the prevention of all wars [...]';
- '[a] **major objective** is to reduce and even eliminate the causes of mistrust, fear, misunderstanding and miscalculations with regard to relevant military activities and intentions of other States […]';
- '[a] **centrally important task** [...] is to reduce the danger of misunderstanding or miscalculation of military activities, to help to prevent military confrontation as well as covert preparations for the commencement of a war, to reduce risk of surprise attacks and of the outbreak of war by accident; and thereby, finally, […] to enhance security and stability.'

Although being drafted in the context of disarmament, the guidelines depict CBMs in a general way as suitable for deliberations on CBMs for cyberspace. Overall, CBMs aim at reaching a sufficient level of predictability of State behaviour at the international level, and to prevent 'loss of control' over a situation in terms of escalation. Consequently, the ultimate end-state desired of CBMs for cyberspace can be described as:

- a common understanding of acceptable State behaviour in cyberspace, and
- a state of cyber stability in international relations.

Importantly, CBMs for cyberspace cannot respond to all cyber threats as relevant to national cyber security, which, according to most national cyber security strategies,[42] would also include aspects of economically or politically motivated cyber crime (including cyber espionage) conducted by both States and non-State actors. CBMs do not aim to present a kind of 'international cyber security strategy' (although some

39 *The Final Act of the Conference on Security and Cooperation in Europe* (1 August 1975) (Helsinki Declaration), Part 2: *Document on confidence-building measures and certain aspects of security and disarmament*, (1978) 14 ILM 1292.

40 UNGA, *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament,* UN Doc A/S-15/3 (28 May 1988) 28-33 (endorsed by UNGA Res 43/78H, 7 December 1988).

41 ibid 30 (para 2.2.1.), 31 (para 2.2.5. and 2.2.6.) [emphasis added].

42 eg OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* (2012, OECD Digital Economy Papers No 211) 5 <http://dx.doi.org/10.1787/5k8zq92vdgtl-en>.

aspects usually included in national strategies, e.g., law enforcement, are also addressed in certain recommendations on CBMs for cyberspace) and to improve the global cyber security. CBMs address specifically the level of inter-State relations and aim primarily at the prevention of an outbreak of an international armed conflict because of misunderstanding and miscalculation of risk.

Indeed, the danger of misunderstanding or miscalculating the intentions or activities of States is particularly increased in the context of cyberspace, due to the specific characteristics of the internet. As malicious cyber activities are not immediately 'visible' in the usual meaning of the term and are not easily attributable to a specific perpetrator, ambiguity, doubt and suspicion are likely to govern international relations. Therefore, and even more so than in other areas of military activities, risk reduction and stabilisation concerning governmental activities are of the utmost importance for the maintenance of international peace and security. As traditional and proven means of risk reduction and stabilisation by deterrence (through the possibility of retaliation) are not feasible[43] in cyberspace due to the challenge of attribution, tools of preventive diplomacy such as CBMs seem to be a viable solution.

3.2 Challenges of Cyberspace

In the past, CBMs have taken a formal or informal, legal or political, unilateral, bilateral, regional or multilateral nature. With regard to content, they range from establishing hotline-communication lines, through unilateral declarations of no first use of certain weaponry, to legally binding arms control treaties with sophisticated verification and control mechanisms. Thus, the CBM concept shows a high level of elasticity. However, its application to cyberspace is a challenging endeavour. A dedicated study, as elaborated[44] by a UN Governmental Group of Experts (GGE)[45] with regard to another 'space' driven by specific characteristics of technology, namely outer space,[46] is yet to be conducted. With regard to the contents, CBMs for cyberspace surely cannot merely replicate the existing sets of measures developed for nuclear, conventional and other weapons, the detailed presentation of which would certainly exceed the scope of the present analysis.[47]

---

43 cf Eric Sterner, 'Retaliatory Deterrence in Cyberspace' (2011) 5 Strategic Studies Quarterly (1) 62, 66; contra: The President of the United States of America (n 14); Forrest Hare, 'The Significance of Attribution to Cyberspace Coercion: A Political Perspective' in Czosseck, Ottis and Ziolkowski (n 12) 125, 135ff.

44 *Prevention of an Arms Race in Outer Space: Study on the Application of Confidence-Building Measures in Outer Space*, UNGA Res 48/305 (15 October 1993).

45 UNGA Res 45/55B (4 December 1990).

46 cf Andrey Makarov, 'Transparency and Confidence-Building Measures: Their Place and Role in Space Security' in UNIDIR, *Security in Space* (The Next Generation-Conference Report, 31 March – 1 April 2008) 69ff <http://unidir.org/pdf/articles/pdf-art2817.pdf>.

47 cf Lachowski (n 37), as well as UN Office of Disarmament Affairs (n 38), OSCE <http://www.osce.org/fsc/44569>, and OAS <http://www.oas.org/csh/english/csbm.asp>.

Hitherto, the significance of CBMs has been acknowledged in the context of disarmament and arms control.[48] CBMs were particularly meant[49] for facilitating the adoption of disarmament or arms control measures, being thus merely a means to an end. Accordingly, some international treaties contain CBMs.[50] As disarmament or arms control commitments are not feasible with regard to cyberspace (section 2), CBMs for cyberspace cannot be regarded as a means to achieve this end. They must show significance *per se* and present a self-contained (preventive) crisis management mechanism.

Furthermore, CBMs in the traditional disarmament and arms control arena were developed in an environment where States mostly held the monopoly of use of force and were in possession of the majority of the weaponry and other military means relevant to international peace and security. As the capabilities and knowledge necessary for conducting significant malicious cyber activities are globally widespread – also outside the governmental sector – the initial situation for the development of CBMs for cyberspace is very different. At first sight, this statement could be countered by the existence of arms control regimes (namely measures against illicit trade) for light arms and small weapons,[51] which can also be often found in hands of non-State actors. However, the main difference to light arms and small weapons is that States cannot control the production and the quantity of malicious software. Thus, also in this regard, the situation for development of CBMs for cyberspace shows dissimilar features.

For reasons expressed above (section 2), CBMs referring only to the reduction of the existence or limitation of the use of certain weaponry cannot serve as an appropriate scheme for CBMs for cyberspace. In the context of CBMs referring to *specific weaponry*, at first sight, only the traditional[52] CBM regarding the exchange of information on military spending seems transferable. However, offensive cyber capabilities are characterised rather by skills than by the equipment purchased. In the cyber context, this feature minimises the importance of 'military spending', otherwise a significant indicator for the defensive or offensive orientation of a State, as expenditure on the training of hackers is not comparable with the spend on conventional or other armaments. Furthermore, declaring 'military spending' would need to include both funds spent on the development and maintenance of (passive) defensive cyber capabilities and the funds spent on (active) offensive cyber capabilities, leaving such a declaration meaningless in terms of indication of defensive or offensive orientation of a State's military. A

48 eg UNGA Res 59/92 (17 December 2004) preamble.

49 cf n 40.

50 cf Lachowski (n 37) 5.

51 cf UN Office for Disarmament Affairs endeavours with regard to 'Firearms Protocol', 'Programme of Action on small arms - including an Instrument on marking and tracing', and 'Basic Principles on the Use of Force and Firearms by Law Enforcement Officials', <http://www.un.org/disarmament/convarms/SALW/>.

52 cf UN Office for Disarmament Affairs (n 38).

respective separation of funds would not be reasonable as, for example, funds spent on the education of military personnel with regard to current hacking methods can be classified as both, in that it is used to conduct offensive operations and for (passive) cyber defence measures in terms of acquiring knowledge necessary for improvement of the resilience of the own network.

Also, any CBMs referring to geographical areas (for example, agreements on demilitarised zones) are not feasible in the context of cyberspace, due to its global scope. The same applies to operational measures, such as the limitations of military manoeuvres and exercises, due to the possibility of operating covertly in cyberspace. As mentioned above (section 2), also any traditional CBMs requiring verification and control are not suitable.

However, CBMs referring to information sharing and cooperation could serve as a suitable model for measures for cyberspace. A detailed listing of such CBMs was elaborated by the Organisation of American States (OAS) Permanent Council (Committee on Hemispheric Security). The *Consolidated List of Confidence and Security Building Measures*[53] includes 36 such measures (based on three political declarations by the OAS Member States).[54] They refer, *inter alia,* to general cooperation commitments, which would potentially be suitable for adaption in cyberspace, such as:

- exchange of information on the organisation, structure, size and composition of defence and security forces,
- advance notice of military exercises,
- conduct of joint training and exercises between armed forces, and
- defence visit programmes with regard to installations.

If 'translated' to cyberspace, such measures would include:

- exchange of information on the organisation, structure, size, and composition of computer network operations (CNO) units,
- advance notice of live hacking exercises by CNO units,
- conduct of joint training and exercises between CNO units, and
- visits of CNO units and their computer laboratories.

Such measures would, most probably, be difficult to implement because of the unwillingness of States to disclose in detail the level of sophistication of their offensive

53 OAS, Permanent Council, Committee on Hemispheric Security, *Consolidated List of Confidence and Security Building Measures for Reporting according to OAS Resolutions* (15 January 2009) <http://www.oas.org/csh/english/csbmlist.asp#Santiago>.

54 OAS, *Declaration of Santiago on Confidence- and Security-Building Measures* (10 November 1995, OEA/Ser.K/XXIX.2, COSEGRE/doc.18/95 rev 3); *Declaration of San Salvador on Confidence- and Security-Building Measures* (28 February 1998, OEA/Ser.K/XXIX.2, COSEGRE.II/doc.7/98 rev 3); *Declaration by the Experts on Confidence- and Security-Building Measures: Recommendations to the Summit-Mandated Special Conference on Security* (4 February 2003, OEA/Ser.K/XXIX, RESEGRE/doc.4/03 rev 3).

cyber forces, and of the knowledge and abilities of the respective personnel. However, the OAS list contains other measures, which could be of value for cyberspace, such as:

- exchange of defence policy and doctrine papers,
- establishment of national points of contact regarding critical infrastructure protection,
- exchange of information on scientific research, and
- exchange of contacts between students, academics, and experts in defence and security studies.

Another example of comprehensive CBMs is the series of documents developed by the Organization for Security and Co-operation in Europe (OSCE) (the organisation's Forum for Security Co-operation) since 1975. The most recent OSCE CBM document is the *Vienna 2011 Document on Confidence- and Security-Building Measures (CSBMs),*[55] which presents a politically binding commitment from all 57 Member States[56] from Europe, Central Asia and North America. Also this set of CBMs considers –apart from measures relating to weaponry, verification and control – extended information sharing and cooperation measures, comparable to the aforementioned CBMs developed by the OAS.

Thus, CBMs for cyberspace could contain some of the cooperation and information sharing measures as endorsed in existing political commitments referring to non-cyber-specific areas. Additionally, CBMs in form of political declarations, as also contained in traditional disarmament and arms control regimes (e.g., declarations on 'no first use'), are viable in the cyber context. It could, however, prove beneficial to conduct an in-depth analysis of 'lessons identified' as collected during the last decades by armed forces and peace research institutes with regard to nuclear and conventional arms control regimes, in order to consider the general findings during the negotiations of CBMs for cyberspace.

3.3 Current Developments

The endeavours to develop CBMs for cyberspace are mainly taking place within the fora of the UN (3.3.1) and the OSCE (3.3.2). Respective negotiations conducted within the regional organisation Association of South East Asian Nations (ASEAN)[57] and the

55 OSCE, *Vienna 2011 Document on Confidence- and Security-Building Measures (CSBMs)*, Doc No FSC. DOC/1/11 (30 November 2011).

56 idem, 'What is the OSCE?', Factsheet <http://www.osce.org/secretariat/35775>; idem, 'Who We Are', OSCE website <http://www.osce.org/who>.

57 ASEAN, *Chairman's Statement of the 19th ASEAN Regional Forum Phnom Penh, Cambodia* (12 July 2012) 5 <http://aseanregionalforum.asean.org/library/arf-chairmans-statements-and-reports.html>.

informal group G8[58] cannot be presented due to lack of publicly available information. Furthermore, CBMs were agreed upon and are negotiated at a bilateral level (3.3.3). Also, some States have issued unilateral declarations, which show their views on the politically acceptable content of CBMs for cyberspace (3.3.4).

3.3.1 United Nations

Cyber security entered the UN agenda in 1998, when the Russian Federation first introduced a draft resolution titled *Developments in the field of information and telecommunications in the context of international security*[59] in the First Committee of the UN General Assembly (UNGA). Since then, two principal 'streams' can be identified with regard to the work of the UN in the arena of cyber security:

1. the politico-military stream within the UNGA First[60] Committee (Disarmament and International Security), focusing on international security in cyberspace, and
2. the economic stream focusing on infrastructure protection and cyber crime within the UNGA Second[61] (Economic and Financial) Committee and, to a certain extent, within the Third[62] (Social, Humanitarian and Cultural) Committee.[63]

58 cf Federal Republic of Germany (n 19); G8, *Deauville G8 Declaration, Renewed Commitment for Freedom and Democracy* (26-27 May 2011, Deauville, France) para 5 <http://ec.europa.eu/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf>.

59 UNGA Res 53/70 (4 December 1998) (adopted without vote).

60 cf *Developments in the field of information and telecommunications in the context of international security* UNGA Res 53/70 (4 December 1998), 54/49 (1 December 1999), 55/28 (20 November 2000), 56/19 (29 November 2001), 57/53 (22 November 2002), 58/32 (8 December 2003), 59/61 (3 December 2004), 60/45 (8 December 2005), 61/54 (6 December 2006), 62/17 (5 December 2007), 63/37 (2 December 2008), 64/25 (2 December 2009), 65/41 (8 December 2010), 66/24 (2 December 2011), 67/27 (3 December 2012).

61 cf *Creation of a global culture of cybersecurity,* UNGA Res 57/239 (20 December 2002) (proposing nine elements for creating a global culture of cybersecurity, annex), *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* UNGA Res 58/199 (23 December 2003) (proposing eleven elements for protecting critical information infrastructures, annex), and *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, UNGA Res 64/211 (21 December 2009) (proposing 'voluntary self-assessment tool for national efforts to protect critical information infrastructure' of 18 points, annex).

62 cf UNGA Res 55/63 (4 December 2000) and 56/121 (19 December 2001) (combating the criminal misuse of information technologies), 57/239 (20 December 2002) (creation of a global culture of cybersecurity) and 58/199 (23 December 2003) (creation of a global culture of cybersecurity and the protection of critical information infrastructures), 64/211 (21 December 2009) (creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures), 55/63 (22 January 2001) and 56/121 (23 January 2002) (combating the criminal misuse of information technologies), and UNGA Res 63/195 (18 December 2008), 64/179 (18 December 2009), and 65/232 (21 December 2011) (strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular, its technical cooperation capacity). The Third Committee deferred considerations on the subject on the criminal misuse of information technologies, pending work of the Commission on Crime Prevention and Criminal Justice, UNGA Res 56/121 (23 January 2002, para 3).

63 For detailed information see Tim Maurer, 'Cyber Norm Emergence at the United Nations. An Analysis of the Activities at the UN Regarding Cyber-Security' (Harvard University, John F. Kennedy School of Government, Belfer Center for Science and International Affairs, Discussion Paper No 2011-11, September 2011) 20-45.

Since 2004, all in all, six GGEs on cyber-related issues have been established within the UN framework, *inter alia,* on identity-related crime (established in 2004 by the UN's Economic and Social Council), the development of a cyber security agenda (established by the International Telecommunication Union (ITU) in 2007), and on cyber crime in general (open-ended GGE established by the United Nations Office on Drugs and Crime in 2010).[64] Within the area of responsibility of the First Committee, upon a proposal of the Russian Federation of 2001, a Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was convened to discuss the threats, possible cooperation and other issues of international information security. This GGE[65] (2004-2005) failed to reach a consensus and to submit a report. It was followed by a second GGE[66] (2009-2010), which was able to reach an agreement[67] on recommendations for future actions, including the development of CBMs:

> [T]he Group of Governmental Experts considers it useful to recommend further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions: [...]
>
> (ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict,
>
> (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices; [...]
>
> (v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.[68]

A third GGE[69] (2012-2013) was established 'to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including [...] confidence-building measures with regard to information space […].'[70] The group reached consensus and issued a report on 7 June 2013. It includes the following recommendations on CBMs for cyberspace:[71]

---

64 ibid 18.

65 Established upon UNGA Res 58/32 (8 December 2003) para 4.

66 Established upon UNGA Res 60/45 (8 December 2005) para 4.

67 UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (16 July 2010) UN Doc A/65/201 (30 July 2010) 8, para 18.

68 ibid.

69 UNGA Res 66/24 (13 December 2011).

70 ibid para 4.

71 UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (7 June 2013) UN Doc A/68/98 (24 June 2013, reissued for technical reasons on 30 July 2013) para 26.

- voluntary exchange of views and information on national strategies and policies, best practices, decision-making processes, relevant national organisations, and measures to improve international cooperation,
- creation of bilateral, regional and multilateral consultative frameworks for confidence building, e.g., workshops, seminars, and exercises,
- expanded information sharing on ICT security incidents,
- exchanging names and contact information of national points of contact for crisis management, including Computer Emergency Response Teams (CERTs),
- increased cooperation to address security incidents that could affect ICT infrastructures or critical infrastructure, and
- enhanced mechanisms for law enforcement cooperation (with regard to incidents that could otherwise be misinterpreted as hostile State actions).

The report uses the term 'ICT', thus avoiding the controversial terms 'cyberspace' *versus* 'information space', which both include contentious political connotations (section 2). Content-wise, the GGE recommendations address a wide range of cyber threats, including cyber crime and threats to critical infrastructure security (earlier drafts went even further, referring to law enforcement in general and to expanded cooperation on combating the use of ICTs for terrorist purposes). Thus, the CBMs proposal extends beyond the traditional notion of CBMs as a tool of prevention of the outbreak of an international armed conflict (section 3.1) and resembles rather a draft of an 'international cyber security strategy' (under the disguise of CBMs). It therefore appears ambitious, which, at the same time, may challenge the adoption of the proposed CBMs at a wider international level, beyond the 15 States[72] participating in the group. It should be mentioned that the abstract references to cooperation ('increased cooperation', 'enhanced mechanisms') without formulation of specific (confidence building) measures could minimise the significance and practical impact of the proposed CBMs. In contrast to the recommendation of the second GGE, 'finding possibilities to elaborate common terms and definitions' with regard to ICT security was not attempted.

3.3.2 Organization for Security and Co-operation in Europe

The OSCE is an organisation with a considerable experience and a successful history with regard to the development of CBMs in the conventional weapons area. Since 2011, the OSCE has shown a comprehensive[73] approach to cyber security, having previously

72 The GGE consists of members from Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, the UK and the US, cf United Nations Office for Disarmament Affairs website <http://www.un.org/disarmament/topics/informationsecurity/>.

73 OSCE, *Resolution on the Overall Approach of the OSCE to Promoting Cybersecurity* in OSCE, *Resolutions of the OSCE Parliamentary Assembly Adopted at the Twentieth Annual Session, Belgrade, 6 to 10 July 2011* (Doc No AS (11) R E) 18ff.

focused its activities on individual aspects[74] of cyber security, such as combating cyber crime and the use of the internet for terrorist purposes. On 26 April 2012, following a respective resolution of the Parliamentary Assembly of 2011,[75] the OSCE Permanent Council established an open-ended, informal working group under the auspices of the organisation's Security Committee '[t]o elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs'.[76]

According to a document of November 2012 and the last draft version of 31 May 2013, the draft set of CBMs for cyberspace discussed during the process included, for example:[77]

- voluntary exchange of national views on aspects of national and international threats to ICT [this could include views on relevant doctrines, strategies, norms, lessons learned, concepts for operating in cyberspace],
- voluntary information sharing, e.g., about national organisations, programmes, or strategies relevant to ICT security,
- voluntary consultations, in order to reduce risk of conflict resulting from the use of ICT,
- voluntary provision and annual updating of contact data of existing national structures which manage ICT-related incidents and coordinate responses [this could include CERTs, but also the administrative and political level],
- voluntary establishment of measures to ensure rapid communication at policy levels of authority [i.e., communication hotlines between capitals],
- voluntary provision of a list of national terminology relating to ICT security accompanied by explanation or definitions of the terms, and
- voluntary exchange of views as to how to use existing OSCE mechanisms to facilitate communication regarding incidents involving ICT.

The approach of the informal working group, assessed solely on the basis of the aforementioned documents, shows hopeful prospects for a successful accomplishment of the task. The set of draft CBMs uses the term 'ICT', avoiding the controversial terms 'cyberspace' *versus* 'information space'. Additionally, it strongly focuses on

74 OSCE, 'Cyber security: virtual threats, real responses', website <http://www.osce.org/home/76011>.

75 idem (n 73) 19, para 11.

76 idem, Permanent Council, *Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (Decision No 1039, Doc No PC.DEC/1039, 26 April 2012).

77 See United States Mission to the OSCE, *Informal Working Group Established by PC Decision 1039: Revised Draft Set of CBM*s (Doc No PC.DEL/871/Rev.1, 7 November 2012) <http://www.par-anoia.net/assessment/at/OSCE_Reprise/pcdel0871r1%20usa%2c%20draft%20set%20cbms.pdf> (document shared by Anonymous 'intelligence agency' Par:AnoIA). The draft version of 31 May 2013 is not publicly available. Additions in brackets are those of the author.

transparency measures and avoids the aspects of cooperation measures going beyond hotline communications in cases of incidents or consultation, such as enhanced cooperation in law enforcement, which is approached with caution by those States which emphasise the aspect of State sovereignty (and consequently territorial jurisdiction) in cyberspace. It was hoped that consensus on a set of CBMs for cyberspace could be reached by the group in 2012.[78] The results are still awaited.

3.3.3 Bilateral Endeavours

The US and Russia had already entered into discussions about internet security in 2009.[79] According to a joint statement of the Presidents of the US and of Russia, a bilateral agreement on CBMs for cyberspace was concluded between the States in June 2013.[80] It includes:[81]

- establishment of a communication channel and information sharing arrangements between CERTs (for protection of critical information systems),
- authorisation of the use of the direct communications link between the States' Nuclear Risk Reduction Centers (exchange of urgent communications employing around-the-clock staffing at the Department of State in Washington, D.C., and the Ministry of Defence in Moscow),
- establishment of a direct secure voice communications line between the US Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council (to manage potentially dangerous situations arising from events that may carry security threats to, or in the use of, ICTs), and
- creation (within a month) of a bilateral working group on issues of threats to, or in the use of, ICTs in the context of international security (in the framework of the US-Russia Bilateral Presidential Commission).

The exchange of strategic documents and of 'military views on cyberspace operations', which was foreseen during the negotiations (according to an intermediate joint statement[82] of the Parties of 2011) is not included in the set of CBMs, as the Parties exchanged earlier white papers, unclassified military ICT strategies and other relevant

78 OSCE, Permanent Council (n 76).

79 John Markoff and Andrew E Kramer, 'In Shift, U.S. Talks to Russia on Internet Security' *The New York Times* (12 December 2009) <http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0>.

80 The White House, *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building* (17 June 2013) <http://www.whitehouse.gov/the-press-office/2013/06/17/joint-statement-on-a-new-field-of-cooperation-in-confidence-building>.

81 ibid; The White House, *U.S.-Russian Cooperation on Information and Communications Technology Security,* Factsheet (17 June 2013) <http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>.

82 idem, *Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin, U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace* (23 June 2011) <http://www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf>;

studies.[83] The CBMs focus on information exchange at high political and technical (tactical) levels in crisis situations. Hereby, the information exchange could also include, for example, warnings with regard to cyber exercises that might be misperceived as threats.[84] The creation of a working group indicates the prospect of further dialogue on cyber security. The involvement of communication channels at high political levels underlines the importance of the topic for the two States and could support an effective implementation of the agreement.

Talks on cyber security between the US and China are also probably being conducted, as indicated by a Chinese proposal reported in March 2013.[85] Between 2009 and 2012, the US-based Center for Strategic and International Studies and the China Institute of Contemporary International Relations have held six formal meetings on cyber security (accompanied by several informal discussions), called *Sino-U.S. Cybersecurity Dialogue*. The meetings have been attended, beside academics, by a broad range of US and Chinese officials. The goals of the discussions have been, among others, to identify areas of potential cooperation, including CBMs.[86] The content of the discussion series resembles preparations for an official CBMs negotiations process.

3.3.4 Unilateral Declarations

Furthermore, some States have issued unilateral declarations, expressing their views on the possible content of CBMs for cyberspace.

Germany's proposal for CBMs for cyberspace, as posted on the website of the Federal Foreign Office, includes the following key elements:[87]

- transparency measures:
  - exchange of information on applicable international law, on organisational structures, strategies and contact partners,
  - exchange of white papers on military organisations and, where available, doctrines in the cyber sphere, and
  - risk reduction.

83 idem, Factsheet (n 81).

84 Ellen Nakashima, 'U.S. and Russia sign pact to create communication link on cyber security' *The Washington Post* (17 June 2013) <http://articles.washingtonpost.com/2013-06-17/world/40025979_1_cyber-security-pact-homeland-security>.

85 Terril Yue Jones, 'China says willing to discuss cyber security with the U.S.' *Reuters* (12 March 2013) <http://www.reuters.com/article/2013/03/12/us-usa-china-cybersecurity-idUSBRE92A0XO20130312>.

86 China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS), *Joint Statement. Bilateral Discussions on Cooperation in Cybersecurity* (June 2012) 1 <http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf>.

87 Federal Republic of Germany (n 19).

- stability measures:
  - establishment or consolidation of crisis communication channels,
  - establishment of CERTs and necessary procedures for exchange, and
  - joint cyber exercises.

More detailed sets of CBMs have been issued by the Russian Federation. The *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* of 2011 commits the armed forces to support [the Russian Federation in] the development of CBMs in the sphere of the military use of information space. The measures proposed in the document include:[88]

- exchange of national concepts for ensuring security in the information space,
- timely exchange of information regarding crisis events and threats in the information space and measures taken with respect to their settlement and neutralisation, and
- consultations on the issues of activity in the information space, which may cause the parties concern, and the cooperation regarding the settlement of any conflict situations of military character.

The focus point here is on the (voluntary) information exchange necessary for actual, preventive and even precautionary crisis management, and on consultation (referring to concepts securing cyber security, information exchange concerning cyber threats and respective measures to their settlement and neutralisation). During a conference in 2012, a Russian representative presented a longer list of potential CBMs, adding to the aforementioned list the following aspects not specific to the armed forces:[89]

- harmonisation of national legislation in order to ensure information safety,
- elaboration of a universal glossary of international information security terms, and
- development of a system of international cooperation among law enforcement agencies with a view to preventing crime in the information sphere.

This longer list of possible CBMs for cyberspace not only indicates an approach towards Russia's Western negotiation partners, e.g., concerning law enforcement cooperation, but also exceeds all expectations for currently negotiated sets of CBMs by proposing 'harmonisation of national legislation' with regard to cyber security; a proposal which is very ambitious. Additionally, the proposal to elaborate a universal glossary of ICT terms reflects the recommendation of the second GGE of 2010 (section 3.3.1).

88 Russian Federation (n 8) 12ff.

89 Fedosov (n 4).

3.3.5 Assessment

All in all, a comparison of the abovementioned sets of CBMs for cyberspace with a list of 'traditional' CBMs, as developed, say, within OSCE or OAS in the context of traditional disarmament and arms control, clearly shows that CBMs for cyberspace, as currently discussed, present a minimum of possible political commitments. It reflects the level of controversy surrounding governmental cyber activities, and might additionally be affected by the different levels of sophistication of States with regard to the development of cyber infrastructure, the governmental use of ICTs, and the national cyber security framework in terms of, for example, the existence of telecommunication regulations and other relevant legislation, cyber crisis management mechanisms, or the existence of a governmental or national CERT.

However, there might be value in the elaboration of the first sets of CBMs for cyberspace, which can serve as a basis for future developments in that arena. It should be mentioned that, surprisingly, the current developments of CBMs for cyberspace, as far as the respective documents are publicly available, do not contain any reference to exchange of scientific research or of academic personnel (as, e.g., endorsed in the OAS-CBMs), a measure, which could be considered as politically rather innocuous.

3.4 Nature of the Commitments

Both the nature of potential CBMs for cyberspace as a political commitment as well as their geographical scope are both predisposed by the unique characteristics of the internet.

3.4.1 Politically Binding *versus* Legally Binding

As mentioned above (section 2), due to political and ideological differences within the international community, there is little prospect for a comprehensive, legally binding regime for cyberspace. CBMs, on the contrary, require an agreement on process rather than on values, and therefore present a more realistic approach to creating an international framework for State behaviour in cyberspace.[90] As mentioned above (section 3.2), CBMs can have a nature of either a political commitment or a legally binding obligation; the latter endorsed within specific arms control treaties, or in specific crisis prevention agreements[91] for the military sector. However, for the following reasons, legally binding CBMs are not feasible in the context of cyberspace.

---

90 cf Lewis (n 15) 59.

91 eg *Agreement On The Prevention Of Dangerous Military Activities* concluded between the US and the USSR on 12 June 1989 (in force since 1 January 1990, 1566 UNTS, Reg No. I-27309) and between Canada and USSR on 10 May 1991 (in force since 10 November 1991, 1852 UNTS Reg No. I-31540), or *Agreement on the Prevention of Incidents On and Over the Waters Outside the Limits of the Territorial Sea of 25 May 1972, As Amended by the 1973 Protocol to the Agreement and the 1998 Exchange of Diplomatic Notes* between the US and the USSR (all in force with the successor Russian Federation).

The value of legal obligations of States in international relations is, *inter alia,* the possibility to 'retaliate' for the breach of said obligations in a legal manner by recourse to countermeasures (i.e., otherwise illegal acts undertaken in response to a previous internationally wrongful act of another State),[92] or by recourse to the jurisdiction of the International Court of Justice (ICJ) or (*ad hoc*) arbitration tribunals. Such legal remedies, however, require a clear attribution of the act which allegedly breaches the legal obligation in question, to a State. In the context of cyberspace, questions of attribution, and thus of State responsibility, should be based on a threefold concept, including (1) technical, (2) legal and (3) political aspects:

(1) Due to diverse technical possibilities, the attribution of malicious cyber activities of a sophisticated nature to a specific IT-system will, despite contrary allegations, as for example, by the recent Mandiant APT1 report,[93] most often be difficult, if not impossible. Hackers predominantly act anonymously, e.g., by modifying network information ('netting'[94], 'DNS-blackholing'[95] etc.) or by choosing a multitude of different and complex routes for their IP addresses[96] and other technical information[97] the computer sends during an internet session. Additionally, the malicious data stream can be encrypted and conducted through a chain of numerous computers belonging to innocent individuals, showing one of them as the source of the malicious activities. Thus, even after an extensive forensic analysis of the malicious data stream, the identification of the computer system the activities originated from, and pinpointing its geographical location, can seldom be affirmed with utmost certainty.

92 eg Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press 1963) 281ff.

93 The report of the US-based information security company Mandiant of February 2013 claims the attribution of malicious cyber activities conducted against IT systems and computer networks based in the US to China's government. The report was widely criticised within the cyber security community for its analytic flaws and 'expectation bias'. See *Mandiant, APT1 – Exposing One of China's Espionage Units* (Report, February 2013) <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>; see critical analysis, eg, Jeffrey Carr, 'Mandiant APT1 Report Has Analytical Flaws', blog (19 February 2013) <http://jeffreycarr.blogspot.com/2013/02/mandint-apt1-report-has-critical.html>.

94 ie manipulating with the network address translation process.

95 ie assigning a domain name system (DNS) information to a false Internet Protocol (IP) address.

96 An IP address (Internet Protocol number) is a 12 digit number identifying a computer or other network device during an internet session. An IP data package is the basic element of data transmission via the internet. It comprises of a header (information on the source, destination, status and fragmentation of the transmitted data) and a payload (transmitted data).

97 eg Media Access Control address or Airport ID for Apple operating systems (order of numbers identifying hardware); Address Resolution Protocol (assignment of a MAC address or Airport ID to an IP address); Service Set Identity (network name); Wired Equivalent Privacy Protocol (coded details about the network); as well as details on the adjustments of the operating system. These details are, if not blocked, automatically transferred during the internet session to any computer requesting this information by a so-called PING (Packet InterNet Grouper). A PING is computer software sending an ICMP-Echo-Request data package to the destination address of the host which is to be scanned, ie, to the IP address, to the Domain Name System name (DNS name) or to the Network Basic Input Output System name (NetBIOS name) of the targeted computer. The targeted system automatically responds by an ICMP-Echo-Reply if, according to the usual adjustments of the system, the system supports the ICMP package.

(2) The legal attribution is based upon the technical attribution. Even if the technical attribution could affirm a specific computer system as the one from which the malicious cyber activities originated, the legal attribution would require evidence (i.e., reliable and unclassified intelligence) about the person or persons involved in the preparation and/or conduct of the activities in question, and about their relationship to a State. The latter, in general terms, would imply that the persons acting were State organs (or otherwise exercising State authority), or acting, 'on the instructions of, or under the direction or control of' a State (see Articles 4-11 of the *Draft Articles on Responsibility of States for Internationally Wrongful Acts*[98] of the International Law Commission (ILC)). It should be mentioned that the issue of State responsibility is a subject of judicial and scholarly controversy (especially with regard to the question whether 'control' is to be deemed as 'overall' or 'effective' control) and respective information on such matters presenting clear evidence is surely not easy to obtain.

As a general rule, international judges have wide-ranging discretion in the assessment of evidence (the principle of free assessment of evidence).[99] Although international courts and tribunals do employ[100] 'presumptions of fact' as an established tool of legal reasoning (not evidence), and the standard of *prima facie*[101] as evidence, legal attribution based solely on the context ('suggestive evidence', 'circumstantial evidence' or 'indication') is not sufficient within the context of attribution in legal terms. This was confirmed by the jurisprudence of the ICJ in the cases *Nicaragua*[102] and *Oil Platforms*.[103] Thus, for example, an analysis of 'behaviour-based algorithms', as partly claimed[104] to support the identification of the originator of malicious cyber activities, is to be deemed as a mere indication (of a rather weak nature), as behavioural patterns (or 'hacking techniques'), as used in certain geographical regions by governmental intelligence agencies, can be imitated in order to intentionally provide a misleading trail.

All in all, despite the interdependency between public international law and international politics, international law contains evidentiary rules, which cannot

98 UNGA Res 56/83 (12 December 2001) annex.

99 *Military and Paramilitary Activities in and against Nicaragua,* Merits (1986) ICJ Rep 14, para 60 ('[...] within the limits of its Statute and Rules, it [the ICJ] has freedom in estimating the value of the various elements of evidence.').

100 Rüdiger Wolfrum, 'International Courts and Tribunals, Evidence' in MPEPIL (n 1) MN 67.

101 ibid 78.

102 *Nicaragua* (n 99) 109 ('Yet despite the heavy subsidies and other support provided to them by the United States, there is no clear evidence of the United States having actually exercised such a degree of control in all fields so as to justify treating the *contras* as acting on its behalf.' [emphasis added]).

103 *Oil Platforms,* Merits (2003) ICJ Rep 161, para 59.

104 eg US Department of Defense, *Cyberspace Policy Report,* Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 (November 2011) 4.

be replaced by political considerations, indications ('circumstantial attribution') or suspicions.

(3) Political attribution displays, in a way, less strict standards, offering the possibility to interpret malicious cyber activities in the context of the overall political situation, and to make use of concepts such as the *cui bono* test. Such an attribution would surely need to be based on a thorough political analysis, going beyond mere suspicions and the usual concepts of 'the enemy'. However, political attribution alone, being 'circumstantial', would certainly not be sufficient in the context of attribution of a treaty breach or other internationally wrongful act to a State in the context of international law, although it presents a perfectly sufficient basis for carrying out political and diplomatic remedies.

The attribution of a treaty breach or an otherwise internationally wrongful act to a State would require proof of technical and legal attribution, whereas the political attribution could serve as a supporting argument only. The lack of technical and legal attribution of malicious cyber activities to a State, which, in practice, is highly probable, will make any allegation of a treaty violation impossible, and thus any treaty-based obligation futile. To quote a grand lawyer: 'Anonymity is a norm destroyer'.[105] Political imputation, based on circumstances and indices, bears the risk of misjudgement, misinterpretation and thereby inappropriate escalation; aspects that CBMs aim to prevent (section 3.1).

It should be mentioned that the lack of attribution or evidence establishing State responsibility is not a new challenge to public international law. In the context of international environmental law, the natural environment being another global resource like the internet, pollution can spread across State borders without (immediate) attribution of the source of the contamination. As a reaction to this, the customary principles of prevention and precaution, including early warning, (*post factum*) information sharing, etc., have been developed.[106] Several of those principles are also aspects considered in the above-mentioned sets of CBMs for cyberspace (section 3.3).

A further argument supporting the development of CBMs as political commitments is of a rather practical nature. Creating a list of politically binding measures has a better chance of success than creating 'hard law' obligations, as the process of treaty negotiations usually takes many years and bears the risk that technical developments overtake the treaty drafting process.

105 Goldsmith (n 13) 12.

106 cf Günther Handl, 'Transboundary Impact' in Daniel Bodansky, Jutta Brunnée and Ellen Hey (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007) 531, 538ff; *Gabčikovo-Nagymaros Project*, Judgement (1997) ICJ Rep 7, para 53; *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion (1996) ICJ Rep 226, para 29.

Accordingly, the international community focuses current diplomatic endeavours on the development of CBMs for cyberspace as politically binding commitments.[107] This, however, does not diminish the practical value of CBMs. Declaratory statements of States are a powerful tool of international politics, and can define acceptable behaviour and de-escalation mechanisms in inter-State relations. Again, a glance at the existing arms control and disarmament regime shows that politically binding commitments present a practicable and effective alternative to legally binding obligations as, for example, in the case of the *Hague Code of Conduct against Ballistic Missile Proliferation*[108] of 2002, or the two sets of guidelines[109] of the Nuclear Suppliers Group of 1978 and 1992 (subsequently amended).

3.4.2 Regional *versus* Global

Given the potential difficulties in agreeing a set of CBMs for cyberspace on the wider international level, the question arises as to whether such measures should rather be developed, negotiated and endorsed at a regional level.

On the one hand, a regional approach could have a better chance of success, as multiple regional characteristics,[110] such as the level of modernity of critical infrastructure systems, specific political relations between neighbouring States, history and, finally, yet importantly, mentality could be considered in a more suitable manner. Additionally, a common understanding and notion of threat is also usually easier to achieve in regional agreements.[111] Finally, the development of regional CBMs would correspond with the tendency within the disarmament and arms control regime to conclude CBMs for regional and even localised crisis situations, as explicitly encouraged by the OSCE *Vienna Document* of 1999 and 2011 (section 3.2) and recommended by the UN GGE report[112] of 2013 with regard to CBMs for cyberspace (section 3.3.1).[113] On the other hand, a global approach to CBMs for cyberspace is, if achievable, rather appropriate, as the internet is a global resource and cyber threats are thus challenges of a global nature. On a rather conceptual level, this finding is supported by the multitude of theories of interdependence in international relations and the sociology of globalisation.[114]

---

107 See Hague (n 32).

108 The HCOC is the only multilateral transparency and confidence building instrument concerning the spread of ballistic missiles. Currently 134 States subscribed to the code, cf <http://www.hcoc.at>.

109 *Guidelines for Nuclear Transfers* of 1978 and *Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software, and Related Technology* of 1992 (both subsequently amended).

110 On different cyber profiles of States see Choucri (n 13) 92-124.

111 cf UN Office for Disarmament Affairs (n 38).

112 UNGA (n 71) para 27.

113 cf Lachowski (n 37) 11-14.

114 For a discussion of 'regionalism' in international relations and international legal policy see International Law Commission (ILC), *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law* (Report of the Study Group of the International Law Commission, finalized by Martti Koskenniemi, UN Doc No A/CN.4/L.682, 13 April 2006) para 85.

As mentioned above (section 3.3), apart from the nearly universal UN organisation and a few particular bilateral endeavours, there are two regional organisations, namely OSCE and ASEAN, which are currently working on the development of CBMs for cyberspace. This, however, does not indicate a general tendency within the international community to develop CBMs for cyberspace at a regional level. The OSCE considers itself a regional (security) organisation (in the meaning of Chapter VIII of the *Charter of the United Nations*). However, the organisation can hardly be deemed regional in geographical terms, as it comprises 57 States from Europe, Central Asia and North America, reaching 'from Vancouver to Vladivostok'.[115] The ASEAN Member States, although, 'shar[ing] the view that regional CBMs should take into consideration the characteristics of the region',[116] decided in 2011 at an ASEAN Regional Forum (ARF) conference that, in future, ARF would work together with OSCE on developing CBMs for global cyber security.[117]

3.5 Obstacles and Challenges for CBMs for Cyberspace

Based solely on the specific characteristics of the internet, several obstacles and challenges for the effectiveness of CBMs for cyberspace can be identified.

Most importantly, anonymity of action in cyberspace, identified above as rendering any legal obligation of States *de facto* futile (section 3.4.1), could at first sight also inhibit the effectiveness of political commitments. The possibility of conducting covert governmental cyber operations seems as potentially minimising the political risk of States to an extreme, and therefore increasing the risk of misperception and improper response to malicious cyber activities. Indeed, despite all political endeavours, and against the background of technological possibilities to act anonymously in the internet, States can retain a high degree of deniability with regard to their cyber activities. Additionally, activities and intentions of States with regard to their cyber capabilities are characterised by a high level of secrecy. From a rather sceptical point of view, as taken by one author,[118] this could result in the ineffectiveness of any transparency measures, e.g., the exchange of (actual) military concepts or of any other significant information. Thereby, the confidence aspect of CBMs, and thus the core aims and purposes of the respective commitments, would prove *de facto* to be in vain. However, this position does not distinguish between trust (or confidence) and assurance, the latter of which, according to sociological and philosophical studies, occurs in situations where

115 OSCE (n 56).

116 Kwon Haeryong, *The ARF Perspective on TCBMs: Future Work* (UNIDIR, Cyber Security Conference 2012: The Role of Confidence Building Measures in Assuring Cyber Stability, Geneva, 8–9 November 2012) slide 6 <http://www.unidir.ch/files/conferences/pdfs/pdf-conf1912.pdf>.

117 Federal Republic of Germany (n 19).

118 Lewis (n 15) 12 and 55.

risk of disappointment is low.[119] (Online) Trust of a higher intensity occurs especially in situations where assurance is low and risk of disappointment is high, i.e., in less structured environments; a finding which provides a compelling argument against the idea that online trust needs a constraining background of norms and commonly shared values to emerge.[120] Additionally, trust, as opposed to assurance, is a facilitator[121] in social interactions; a notion which can also be applied to inter-State relations. Thus, anonymity, which prevents effective deterrence as well as legal 'retaliation', and which is one of the reasons for the development of CBMs for cyberspace, can be deemed at the same time as the very reason for the establishment of trusting relationships between States. All in all, the trust (or confidence) can only be considered futile if it is disappointed by certain behaviour.

Furthermore, the concept of CBMs for cyberspace does not embrace the notion that malicious cyber tools are foremost an asymmetric means of power. Malicious software is a powerful tool in the hands of 'super-empowered angry individuals' (freely adapted from Samuel Huntington's *The Clash of Civilisations*).[122] It will be difficult to prevent 'loss of control' and to de-escalate any stand towards other States in a situation of a cyber crisis (supposedly) caused by determined, and most probably anonymously acting non-State actors. Cyber tools are also the perfect means in the hands of politically unstable States which are otherwise militarily inferior. These States are potential risk factors for international peace and security in the context of cyberspace, given that cyber tools are a relatively powerful and comparatively inexpensive means that can be obtained on demand. It could prove disadvantageous to disregard such potential within the context of development of CBMs for cyberspace with regard to negotiation partners (e.g., focusing on 'like-minded' States).

Finally, despite the unique characteristics of the internet, the concept of CBMs for cyberspace has not yet approached the notion of considering the potential of de-escalation of certain non-State actors in a cyber crisis situation. CBMs aim to prevent the outbreak of an international armed conflict through 'loss of control' and inappropriate escalation of a cyber crisis situation, by establishing practical measures and processes of (preventive) cyber crisis management between States. This notion is rightly based on the reasoning that an international armed conflict can exist between States only. Consequently, negotiations of practical measures aiming to prevent an international armed conflict would be a matter of inter-State relations, excluding any consideration of the de-escalation potential of non-State actors. However, this traditional notion does not fully appreciate the unique characteristics of the internet, the probabilities of

119 cf Matteo Turilli, Antonino Vaccaro and Mariarosaria Taddeo, 'The case of on-line trust' (2010) 23 Knowledge Technology and Policy Journal (3-4) 338ff.

120 ibid 339.

121 ibid 342.

122 cf Choucri (n 13) 226ff.

cyber crisis scenarios and realities of the global cyberspace, which is shaped, driven and managed mainly by non-State actors. Data streams sent from computer systems located on a foreign State's territory, entering through technical components located on the State's own territory (being further transferred, e.g., to governmental, including military, networks) are managed by so-called tier 1 internet service providers (ISPs). In most developed democratic States, tier 1 ISPs are privately owned. These companies are the actors who would probably first notice damaging data streams of an intensity and quality relevant to national security, and undertake practical crisis management measures. Therefore, being the 'gate' for international interaction in data transmission, the role and practical de-escalation potential of tier 1 ISPs (e.g., technical information exchange with other States' tier 1 ISPs) could prove most valuable in the context of practical measures of international cyber crisis management. On the opposite end of the scale, an 'isolatory' approach at the international political level, disregarding the above-mentioned potential of non-State actors, could eventually render international cyber crisis management ineffective, and shift it *de facto* to the technical level, especially to global, informal cooperation fora, e.g., the Forum of Incident Response and Security Teams (FIRST).[123]

4. Significance of Political Commitments for International Law

As explained above (section 3.4.1), the international community is currently focusing its diplomatic endeavours on the development of CBMs for cyberspace of a politically binding nature. The value of political declarations should not be underestimated. In terms of practice, they can influence State behaviour in a powerful way. Apart from this, political commitments have some significance for international law.

There has always been a certain interdependency between policy and law. This is especially apparent in public international law, where States create norms by their behaviour in international relations, *inter alia,* by generally uniform and consistent practice accompanied by respective *opinio iuris*[124] (international customary law)[125]. The political discourse within the international community in the process of finding consensus for a joint political declaration can support the development of *opinio iuris* of the States. Therefore, negotiations preceding the formulation of political declarations,

123 FIRST is a global network of computer security incident response and security teams from government, commercial, and educational organisations that work together voluntarily to deal with computer security problems and their prevention, see further information at <http://www.first.org/>.

124 *Opinio juris* refers to the belief of States that a certain State practice is permitted or required under international law. *Opinio juris* is an aspect necessary for the development of international customary law, cf Malcolm N Shaw, *International Law* (6th edn, Cambridge University Press 2008) 84ff; Rüdiger Wolfrum, 'Sources of International Law' in MPEPIL (n 1) MN 25.

125 cf Wolfrum (n 124) 25; Tullio Treves, 'Customary International Law' in MPEPIL (n 1) MN 17ff (with references to ICJ jurisprudence); James Crawford, *Brownlie's Principles of Public International Law* (8th edn, Oxford University Press 2012) 23-30 (detailed discussion of the elements of customary international law); *North Sea Continental Shelf,* Judgement (1969) ICJ Rep 3, para 77.

as well as the declarations *per se,* can support the development of future norms of customary international law.[126]

Furthermore, political declarations, especially when broadly supported within the international community, can support clarifying the content of international law norms of a rather general character, thus being a supportive means for the purposive interpretation of law.

In the context of CBMs for cyberspace, which are discussed at the international level as a substitute[127] for legally binding obligations, the concept of so-called 'soft law' becomes relevant. 'Soft law' comprises (apart from the category of resolutions of international organisations) non-binding agreements between States.[128] It can emerge when the international community identifies the need for regulation; however, reaching a comprehensive consensus resulting in the development of a legal norm (conventional or customary international law) seems not to be successful.[129] 'Soft law' is a practical means in international relations to fill such a gap. Being 'in the twilight between law and politics',[130] 'soft law' is described in scholarly writings as showing a certain proximity to law, and having the capacity to produce certain legal effects by shaping common expectations concerning State conduct in international relations (in terms of the principles of good faith and estoppel[131]).[132] Furthermore, 'soft law' has the benefit that rules which are not legally binding can first prove their value and practicability within international relations before becoming a 'hard law' obligation.[133] It should be mentioned that some scholars are sceptical of the 'soft law' concept because of the risk of blurring the line between law and political commitments.[134] Convincingly, it is asserted that 'soft law' is only of a speculative nature *ex ante*, and can be of value only *ex post*, explaining the evolution of a certain norm of international conventional or customary law.[135] However, *ex ante* 'soft law' can be also useful as a means of a purposive interpretation of international law.[136]

126 cf Wolfrum (n 124) 63.

127 See Hague (n 32).

128 Categorisation according to Daniel Thürer, 'Soft Law' in MPEPIL (n 1) MN 10-17.

129 Wolff Heintschel von Heinegg, 'Die weiteren Quellen des Völkerrechts' in Knut Ipsen (ed), *Völkerrecht* (6th edn, CH Beck, 2010) § 20 MN 21.

130 Thürer (n 128) ch. I.

131 Principle of non-contradiction of their own conduct (*non licet venire contra factum proprium* or *allegans contraria non audiendus est*); see Oscar Schachter, 'The Twilight Existence of Nonbinding International Agreements' (1977) 71 American Journal of International Law (2) 296ff. For references to international courts' application of the principle of estoppel see Thomas Cottier and Jörg Paul Müller, 'Estoppel' in MPEPIL (n 1).

132 Thürer (n 128) 9, 27-28.

133 ibid.

134 Heintschel von Heinegg (n 129) § 20 MN 22; Wolfrum (n 124) 63.

135 ibid.

136 cf Thürer (n 128) 29.

CBMs for cyberspace, as a political declaration or even 'soft law', will certainly support the interpretation of public international law as applicable to cyberspace.

5. Summary and Conclusions

The use of Cold War metaphors with regard to cyberspace appear as a facet of nostalgia for the bipolar, relatively predictable political environment of those times, where 'fronts' were apparent and concepts of the enemy clear. In the cyber context, any simple recipe would fail, facing as it would the complex realities of today's world, where cyber tools empower non-State actors and politically unstable and otherwise militarily inferior States. Herewith, the usual search for power balance between the global players, which traditionally would lead to relative security in international relations, is not useful, as cyberspace has the potential to empower the weak ones and leaves the technically advanced 'great powers' particularly vulnerable. For diverse reasons, as demonstrated in the present chapter, the adoption of an arms control regime for cyber means or the conclusion of an international agreement on State behaviour in cyberspace are at the present neither practicable nor politically feasible. Against this background, the elaboration and adoption of CBMs for cyberspace is the viable option, as such measures focus rather on process than on values.

Due to specific characteristics of the internet, traditional CBMs referring to specific weapons, to geographic areas (of demilitarisation), to limitations of military manoeuvres or to any kind of verification and control are not feasible. Also, CBMs referring to military spending, otherwise a useful indicator for the defensive or offensive orientation of a State, are not practicable in the cyber realm, as cyber capabilities are characterised by skills and knowledge rather than the equipment purchased. Moreover, the situation for the development of CBMs for cyberspace is very different from the environment, in which traditional disarmament negotiations take place, as States do not have the monopoly or control over production and import of malicious software.

Thus, CBMs which predominantly refer to transparency (information sharing) and cooperation would be the most feasible option of CBMs for cyberspace. A comparison of the presented sets of CBMs for cyberspace with 'traditional' CBMs referring to transparency and cooperation clearly shows that CBMs for cyberspace, as adopted, recommended or currently drafted, present a minimum of possible political commitments. This reflects the level of controversy surrounding governmental cyber activities, and might additionally be affected by the different levels of sophistication of States with regard to the development of cyber infrastructure, national cyber security framework, and the role cyberspace plays in administration, industry and civil society. However, there might be separate value in the fact of the elaboration of the first sets of CBMs for cyberspace, which can serve as a basis for future developments in that arena.

The value of legal obligations is the possibility to take legal remedies (such as countermeasures) in cases of their breach which, in any case, requires a clear attribution of the supposed violation of the norm to a State. Attribution, of which a threefold concept was presented in this chapter, will very seldom occur in a form which would satisfy the evidentiary rules of international law. As the lack of attribution would make any allegation of a treaty breach impossible, and thus any treaty-based obligation futile, the international community focuses their endeavours on the development of CBMs as politically binding measures.

Political declarations are a powerful tool of international relations, which can have a *de facto* binding character. Furthermore, the political discourse within the international community can support the development of international customary law by facilitating the evolvement of *opinio iuris*, which is (beside State practice) a constitutive aspect of international custom. Furthermore, political declarations can support the interpretation of international law norms of rather general character. Additionally, as CBMs are discussed at the international level as a 'substitute' for legally binding obligations, they could show the character of 'soft law', thus being 'in the twilight between politics and law', and showing some normative value.

The challenge of attribution of malicious cyber activities as well as the secrecy surrounding offensive cyber capabilities of States does not necessarily limit the effectiveness of CBMs as political commitments, as is claimed especially with regard to the 'transparency' aspect of CBMs. Although the anonymity of action within the internet minimises the political risk of States (with regard to political retaliation), sociological and philosophical studies show that, where assurance is low and risk of disappointment is high, trust (as opposed to assurance) tends to show a higher level of intensity. However, one of the obstacles to the effectiveness of CBMs for cyberspace is that malicious cyber tools are foremost an asymmetric and powerful means in the hands of 'super-empowered angry individuals' or politically unstable States which are otherwise militarily inferior. Another impediment is the fact that the adopted, recommended or currently drafted sets of CBMs do not consider the potential of de-escalation of certain non-State actors, such as tier 1 ISPs, who would first notice irregular data streams or malicious software, and undertake crisis management measures. An 'isolationist' approach at the international level could eventually shift the international cyber crisis management to global, informal, technical cooperation fora.

All in all, in preparation for the negotiations of CBMs for cyberspace, it would be useful to conduct an in-depth study on the applicability of CBMs to cyberspace, as elaborated in 1993 in the context of CBMs for outer space. Additionally, an analysis of lessons identified with regard to CBMs, as collected by armed forces and peace research institutes during the last decades, would be beneficial in order to consider the findings during the negotiations with regard to cyberspace.

Liina Areng

International Cyber Crisis Management and Conflict Resolution Mechanisms

1. Introduction

Today, international organisations, as main actors in international crisis management, are faced with complex new issues and a hybrid character of international relations. The world is increasingly multipolar and new actors as well as new challenges emerge at the speed of light.

As states and non-state actors are actively using cyberspace to promote their political agendas or achieve other objectives, it entails a great risk of miscalculation and escalation in inter-state affairs. States with high cyber dependencies – in economic, social, and military terms – are facing common and interlinked challenges, not only from exposure to risks from shared cyberspace and targeted attacks, but also from hazards deriving from critical cross-border dependencies and deep economic ties. According to a recent study by the European Network and Information Security Agency (ENISA), cyber incidents caused by natural disasters, systems failures or human error overwhelmingly exceed the number caused by attacks and other malicious activities, which make up only eight per cent of all cyber incidents.[1] It seems reasonably clear that if cyber problems tend to run across borders, then the containment of the crisis and the consequence management should also follow a cooperative approach.

States and international organisations usually learn through crises. As a result of the troubling examples of the 2007 cyber campaign in Estonia, the 2008 Georgia-Russia conflict and the 2010 Stuxnet virus, a serious worldwide discussion on cyber security has emerged in many regional and international forums. In 2009, the United States (US) Government Accountability Office (GAO) identified 19 global organisations 'whose international activities significantly influence the security and governance of cyberspace.'[2] In 2011, in the speech at the Munich Security Conference, the United Kingdom's (UK) Foreign Minister William Hague stated that over 30 multilateral organisations worldwide are engaged in cyber security issues but that the 'debate is fragmented and lacks focus.'[3] It is obvious that, compared to national efforts to address cyber security, international organisations are more limited in terms of resources and hindered in their actions because of political disagreements. Yet, in 2010, a United Nations (UN) Group of Governmental Experts (GGE), including representatives

1 ENISA, 2012.

2 GAO, 2010.

3 Hague, 2011.

from 15 states, among them China, India, Russia, and the US, stated in its consensus report that 'existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century.' The perception of new national security risks seems to have created a stronger appetite for some multilateral arrangements for securing cyberspace and preventing conflict. A natural element of this national security logic should also be cooperative engagements for conflict resolution and crisis management.

This chapter will explore how existing international organisations approach cyber challenges, what mechanisms are available, and what trends can be identified in connection with developing international policy responses to cyber emergencies. The analysis focuses only on international organisations; any other multilateral or bilateral arrangements between states are beyond the scope of this chapter.

2. Tools and Challenges of International Cyber Crisis Management and Conflict Resolution

International relations practice is not confined to legal processes and rules of evidence. Most international conflict resolution is political; organisations settle disagreements by diplomatic rather than strict legal means.[4] Even the threat of taking strong action should dissuade states from conducting harmful cyber activities against other states and force governments to constrain malicious non-state actors resident in their territory.

Since crisis management is traditionally a state-to-state affair, states are unavoidably important actors also in cyber conflict de-escalation. The unexpectedly large consensus at the World Conference on International Telecommunications (WCIT) in Dubai in December 2012 on imposing stricter inter-state regulation of the internet shows that cyberspace is no longer 'borderless'. The notion of internet as 'commons' is forgotten as nations actively exercise their sovereignty to apply their laws within their borders. Although it may be difficult to identify the perpetrator behind malicious cyber activities, it is possible to identify the perpetrator's 'host nation' and to hold that state responsible for harmful activities coming from its territory. State obligations are clearly described in the Council of Europe *Convention on Cybercrime* that confirms the jurisdiction of states over any offence committed in their territory.[5] The UN General Assembly issued a resolution in 2001 on combating criminal misuse of information technologies, calling upon member states to prevent their territories from being used as safe havens for actors misusing information technology, and to cooperate in the investigation and prosecution of such cases.[6] The reaction of the international community to the September 11 attacks established a 'fundamental shift from the state responsibility standard of effective

4 Klabbers, 2009: 240.

5 Council of Europe Convention on Cybercrime, CETS No 185, Article 22.

6 UNGA, A/RES/55/63, 2001.

control to one of "indirect responsibility"".[7] This means that a state has responsibility for the actions of non-state actors that use its territory to launch attacks on other states, and that a state which fails to meet its international obligation to prevent such attacks has failed in that obligation.[8] Governments are publicly naming such states on the basis of 'reasonable evidence'. The US Department of Defence's 2013 Annual Report to Congress on China accuses the Chinese government and the People's Liberation Army of carrying out targeted cyber intrusions against US government and industry.[9] Similarly, the Chinese Ministry of National Defence blames the US for the majority of the cyber attacks against its military networks.[10]

Traditional crisis management instruments range from observers and arbitrators to civilian crisis management and peacekeeping. Do cyber emergencies differ, and is there a need for new tools? The usual containment and de-escalation mechanisms such as military intervention, arbitration, diplomatic tools or economic 'motivators' – economic opportunities or sanctions – seem to apply in cyber crisis as well as more traditional crises, depending on the specific political context and severity of the consequences. One particular aspect of cyber emergencies is the time factor, both in terms of early warning and escalation. In cyber conflicts, since an adversary's preparatory phase is either very short or hard to detect, the attacks may come with no forewarning, which for unprepared or significantly underprepared organisations means that crisis can escalate very fast. If the victim state has the ability and will to retaliate, a single incident could rapidly grow and escalate to full-scale warfare involving not only the initial aggressor and the victim, but potentially a crowd of sympathisers within and outside of the parties of conflict. Cyber crisis is thus a complex issue for conflict de-escalation, as it requires rapid containment efforts and the coordinated cooperation and involvement of a wide array of stakeholders, including military and intelligence agencies, the private sector, and civil society, each of which has a different organisational culture and different interests.

Modern crisis management also uses several new tools. Social media has become an increasingly important warning and information instrument during natural disasters, providing an avenue for alerts, real-time updates, and information about shelters, road closures etc. Automated text messaging is also used to communicate between government agencies and the public. In cyber emergencies these instruments can also be used to receive alerts and warnings as well as to curtail escalation, but social media can also be exploited by the adversary and become part of the cyber conflict.

7 Graham, 2010.

8 Becker, 2006.

9 'In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military' US DoD Report to Congress, 2013.

10 Whitney, 2013.

Anticipatory measures that consist of ensuring adequate protection of critical national cyber assets and early warning are vital for ensuring better preparedness for cyber emergencies. Sharing of best practices among states and capacity building in less capable countries can contribute to resilience building, both technical and organisational, as well as facilitate and accelerate crisis response. National and multinational exercises help to test procedures and identify important communication and escalation gaps.

It is clear that, in order to achieve good national cyber security, domestic efforts need to be complemented by strong international cooperation. It is also obvious that international arrangements cannot be effective unless each state makes sufficient investment into securing its own networks. The drive by some nations towards stronger international cooperation and pledges to help the less advanced, driven by interdependencies and mutual vulnerabilities, should not allow the less aware or less resourceful nations to become free riders. Nations that do not have adequate legislative and institutional frameworks in place to protect their cyber assets are less likely to receive assistance from other states because 'in a rapid reaction situation an existing procedure better supports effective interaction and because there is a certain amount of 'homework' that can and needs to be done primarily by the victim.'[11] Having good working relationship between government and the technical community can also facilitate action by national authorities rather than relying on external assistance.

The critical interdependencies and mutual vulnerabilities in cyberspace should encourage cooperation between nations in times of crisis. However, despite the overall interest in discussing cyber security problems, the more specific debate on international cyber crisis management remains largely undeveloped, and states continue to hold competing and often contradictory views about the exact mandate of different organisations in this field, drawing very clear lines between national and international obligations. Countries also differ in the general approach to cyber (e.g., civilian, military, or intelligence-led) and to national cooperation environments (completely voluntary or completely mandated); this creates imbalance and complexity in finding the right counterparts and creating comparable crisis management procedures. Cooperation in cyberspace comes down to trust more than anything, and trust is hard to build. Information sharing and early warning are essential components of crisis prevention and management, but usually require a long history of working together.

Whether any international initiative is successful depends largely on its spokespeople and leaders. If there are sensitive political issues at stake, the more neutral the leader is perceived to be, the more successful the outcome. Most organisations have a strong leader nation which drives development: the Association of South East Asian Nations (ASEAN) has Japan; the Collective Security Treaty Organization (CSTO) has Russia; the Shanghai Cooperation Organisation (SCO) is dominated by Russia and China;

[11] Tikk, 2010.

the North Atlantic Treaty Organization (NATO) and the Organization of American States (OAS) have the US. The International Telecommunication Union (ITU) is considered to be heavily influenced by Russia and China, supported by the fact that ITU's current Secretary-General, Hamadoun Touré, received his education in Russia.[12] Strong leadership can be positive in terms of giving the organisation a push forward and introducing ideas and incentive, but it can also be a source of dispute and mistrust.

Another important factor in cyber crisis management is the language and knowledge gap between the technical/operational and strategic/decision-making levels. Technicians talk to each other in a cryptic language which is incomprehensible to most decision makers. Incomprehension or fear of incompetence leads to ignorance, and cyber crisis management becomes an issue for the 'techies' to solve, until it affects critical sectors of society and the political reputation of decision makers. There are not many senior managers who master the language of information technology to enable swift crisis communication in times of urgency. The communication gap will probably be even more difficult to bridge from bottom-up. Another issue that comes from communication errors and lack of situational awareness in national crisis management hierarchy is inconsistency in cooperative engagements with external entities. The technical experts use their own expert-level communication channels with international counterparts, and may be unaware of or insensitive to national political dilemmas. The result may be that informal technical assistance may go well ahead of the properly endorsed political cooperation.

States are more likely to find incentive for cooperation under international pressure, although positive motivators and friendly assistance can sometimes be a more efficient path in de-escalation of a crisis. A general tendency in international disputes is that instead of threatening coercive measures against states with compliance problems, governments offer them assistance, be it technical or financial, to reach the required standards.[13] Since no common norms and standards for cyber security exist – organisations such as the European Union (EU) and NATO have only recently started discussions on minimal requirements for increased resilience and operational effectiveness – the only time when major national deficiencies are revealed is in times of incidents of national or international significance. Although no such international practice exists yet, it would be reasonable to assume that if a state is unable to contain attacks that traverse its territory or make every effort to minimise their impact on the victim state, other states could render assistance by supporting remedial and response measures rather than by jumping to punitive action.

At the heart of the international crisis management system is the *Charter of the United Nations* (UN Charter) which provides the legal framework for the actions and

12 Blue, 2012.

13 Klabbers, 2009: 247-248.

interactions of states and regional organisations. Chapter VIII foresees a substantial role for regional organisations in conflict management. The UN Security Council has a primary mandate to maintain international peace and security, but in order to deliver security the UN needs to collaborate with a range of regional organisations, since it is perceived that reaching agreement on and the subsequent implementation of specific measures is usually easier at the regional rather than at the global level. However, the ability of regional organisations to deliver varies. The chance of agreement on cooperative measures such as close-to-real-time information sharing and mutual assistance is definitely higher in limited-membership organisations composed of like-minded member states. It is also easier in regions with a long and highly developed tradition of cooperative arrangements, such as the Nordic cooperation between the Scandinavian countries or the so-called Five Eyes agreement on security partnership between the US, UK, Canada, Australia and New Zealand, representing a common linguistic region. In less heterogeneous organisations with varying levels of military, political, and economic power, forming consensus is more difficult unless there is a clear dependency/dominance relationship. A major problem in reaching a cooperative regional solution is likely to be the lack of trust due to past challenges or political or economic competition. And because trust is a fundamental factor in cyber cooperation, cyber threats to national security are more likely to be addressed at a national level or, at best, through bilateral agreements between states.

No two organisations are identical, therefore it is difficult to generalise on the organisations' overall ability to deal with cyber challenges. By examining the functions and capabilities of different global and regional organisations it is possible to describe the multi-actor, multi-issue nature of international cyber crisis management as 'complexity management.'

3. Global Organisations

3.1 United Nations

The UN is the only legitimised authority to generate binding international obligations[14] but it is also an important actor in creating 'soft law' through non-binding recommendations of the General Assembly.[15] Soft law is designed to influence political actors' behaviour and state practice and can gradually become a norm.[16] Since General Assembly resolutions carry much less weight, they also carry much less political burden and have a greater potential to develop into generally accepted practice.

14 UN Charter, Article 25.

15 *Ibid,* Articles 10 and 12.

16 Boyle, 1999.

The UN, because of its global state participation and outreach, could play a dominant role in promoting preparation for, response to and recovery from cyber incidents. Since 1998, when the Russian Federation first introduced a Draft Resolution on 'Developments in the field of information and telecommunication in the context of international security'[17] in the First Committee of the General Assembly, the UN has served as an important forum for debates regarding international cyber security. Despite the fact that the main narrative in the UN discussions has been arms control and confidence building, rather than the non-military end of the threat spectrum, it demonstrates a wider appetite for collective action. Promoting global cyber culture or establishing norms of state behaviour in cyberspace help to create a more transparent and predictable cyber environment where conflict escalation due to miscommunication would be less likely. The UN also focuses on capacity building, which is another important element in raising the level of national crisis management preparedness.

The UN, as a global forum, is also a good venue for nations to air their political differences. The discussions on cyber security have to date largely centred around the political differences between Russia and the US, or the fundamental debate between the necessity of an international treaty on information warfare versus considerations for freedom of expression. This relationship, which started with ignorance, continued with confrontation, and resulted in compromise, is an interesting example of relationship-building through finding the lowest common denominator. This process can be clearly observed through the introduction and sponsorships of General Assembly draft resolutions.

Russia was for seven years the sole sponsor of the resolution, first introduced in 1998. In 2005, the US suddenly decided to vote against it, disrupting the pattern. A great game usually attracts attention and draws in more players, and the following four years (2005-2008) of persistent US opposition to the resolution drew other nations to the game, supporting one side or the other. In 2009, the states co-sponsoring the Russian resolution reached 30. The third major player – China – was quietly observing the Russian-US debate but entered the fray only in 2009, co-sponsoring the Russian resolution for the first time. Finally, in 2010, the US decided to switch sides and negotiated compromise wording, omitting a few controversial elements on common definitions and international principles, joining the group of resolution co-sponsors which had by then reached 36. The increase in importance of the issues over the decade and the wish to contribute to the debate can also be seen in the way in which several UN member states communicated their positions on cyber security in their responses to the UN Secretary-General as a reaction to the work in the First Committee.[18]

17 UNGA A/35/576, 1998.

18 UNODA, 2011: 18-39.

To provide a working level platform for cyber security related debates in the UN, a GGE was set up in 2001 by the General Assembly's First Committee to review existing and potential threats in the field of international information security and possible measures to address them, as well as to examine international concepts aimed at strengthening the security of global information and telecommunications systems.[19] The group, comprising 15 states[20], began its work in 2004 but failed to reach consensus needed to produce a report in 2005. The main reason for this was, according to the Russian delegation, the question of whether international law 'sufficiently [regulates] the security aspects of international relations in cases of 'hostile' use of ICTs [information and communication technologies] for politicomilitary purposes.'[21] The second group began its work in 2009 and finished its discussions in 2010 with a successful report. In his foreword to the report, the UN Secretary-General noted that the 'dialogue among Member States will be essential for developing common perspectives,' and added that 'practical cooperation is also vital, to share best practices, exchange information and build capacity in developing countries, and to reduce the risk of misperception, which could hinder the international community's ability to manage major incidents in cyberspace.'[22]

The five general recommendations from the group were: further dialogue to discuss norms pertaining to state use of ICTs; confidence-building; stability and risk reduction measures; exchange of policies and best practices; and capacity building. The third GGE began its work in 2012 and produced a consensus report in June 2013, which will be presented to the 68th session of the General Assembly and which provides a list of recommendations on the norms, rules, and principles of responsible behaviour by states, confidence building measures and exchange of information, and capacity-building measures. The next logical step on this political trajectory is to agree on some specifics on how to support the implementation of these recommendations; for example the proposal for 'the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery, and mitigation actions,' which would be an effective crisis management tool.[23]

In addition to the First Committee, two other General Assembly Committees have met to discuss draft resolutions pertaining to cyber security.[24] In 2003 and 2004, the General Assembly adopted two resolutions dealing with the creation of a global culture

19 UNGA A/RES/56/19, 2002.

20 Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea, The Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

21 Streltsov, 2007: 6.

22 UNGA A/65/201, 2010.

23 UNGA A/68/98, 2013.

24 Second Committee (Economic and Financial Committee) and Third Committee (Social, Humanitarian and Cultural Committee).

of cyber security and the protection of critical information infrastructures. Resolution A/57/239 of 2003 invites states to 'act in a timely and cooperative manner to prevent, detect and respond to security incidents,' while Resolution A/58/199 of 2004 calls on international organisations and member states 'that have developed strategies to deal with cyber security and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cyber security' and to cooperate in order to 'secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.'[25]

The UN has developed elementary consensus on cyber confidence building and adopted declarative language on the need to cooperate on crisis management and capacity building. Although idealistic language is still far from implementing or even from identifying proper mechanisms to promote such cooperation, it is an important avenue that the UN member states should continue to pursue.

3.2 International Telecommunication Union

The ITU is an international organisation and a UN specialised agency working on a wide range of global issues related to ICT and embracing a wide variety of actors in cyberspace. It differs from classical international organisations because, in addition to governments, it also allows the participation of the private sector and academia. On cyber security, the ITU covers 'practical aspects'[26] through a range of technical and standardisation issues, including developing best practice guides on critical infrastructure protection and capacity building in developing countries. The ITU maintains an international cyber security forum called Global Cyber-Security Agenda, established in 2007 and intended to enable collaboration on enhancing confidence and security in the information society. As a forum to collect best practices, develop tool-kits and make recommendations on advancing national cyber security, the Agenda operates through five work streams: Legal Measures, Technical and Procedural Measures, Organisational Structures, Capacity Building and International Cooperation. A more practical feature is that the ITU collaborates with the International Multilateral Partnership Against Cyber Threats (IMPACT), an international public-private initiative, which focuses on early warning systems and a secure electronic collaboration platform for incident response and guidance on threat mitigation. Its Global Response Centre in Cyberjaya, Malaysia, also maintains a secure environment called ESCAPE for pooling resources and collaboration between cyber experts, including maintaining a catalogue of IT professionals that can

25 UNGA A/RES/57/239, 2003 and A/RES/58/199, 2004.

26 UN CTITF, 2011: 7.

be called on to assist during a crisis. While it is difficult to assess the real practical value of this recent initiative from the outside, it seems to provide a useful coordination and response tool for members during national and international cyber emergencies.

The major issue that brought the ITU to media headlines in December 2012 was the WCIT conference in Dubai, where 89 (out of 144) participating states endorsed a non-binding resolution, submitted by the United Arab Emirates and supported by Russia and China, calling for the ITU 'to foster an enabling environment for the greater growth of the Internet.'[27] In other words it voted to transfer authority for regulating critical aspects of the internet from the Internet Corporation for Assigned Names and Numbers (ICANN) to the ITU. This indicated that an unexpectedly large number of states actually want to see greater state control and inter-state regulation of the internet, allowing governments to manage and restrict the traffic that flows through their networks. Some observers were talking about a 'digital Cold War'[28] and some were so frustrated with the outcome that they even called for the abolition of the ITU.[29] The next high-level negotiations over the ITU's role in internet governance will take place in South Korea in 2014.

4. Regional Organisations

4.1 North Atlantic Treaty Organization

NATO's principal mission is to safeguard the freedom and security of its member states through political and military means. In crisis management, NATO claims to be a regional organisation with a global reach, involving 'military and non-military measures to respond to a threat, be it in a national or an international situation.'[30] NATO is ready to react in case of natural, technological or humanitarian disasters, deciding each engagement on a case-by-case basis. The response mechanisms range from soft measures (diplomacy) to robust military action. All decisions are taken by the principal political decision-making body, the North Atlantic Council (NAC). Each Ally can at any time request under Article 4 of the North Atlantic Treaty to consult and discuss any significant national security issue, 'whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.' There is no automatism in NATO's responses to Allies' requests for assistance pursuant to Article 4; any collective action will be decided as a result of consultation. The Article 4 elements are also represented in the invitation to Partnership for Peace states for crisis consultations and requests for assistance.

27 ITU, 2012.

28 L.S., Babbage – Science and technology blog, 2012.

29 Gordon, 2012.

30 NATO, 'A-Z: Crisis management'.

NATO uses a 'Six-Phase Crisis Management Process' to assess a crisis situation and develop a response. Such a phased approach is primarily designed to allow the relevant staffs and specialised committees[31] to co-ordinate their work and to submit advice to the NAC. It also allows Supreme Allied Commander Europe (SACEUR) sufficient time to undertake preparatory military planning and for capitals to make sound strategic political decisions. The phased approach is not rigid, and, depending on the crisis situation and urgency of response, it is not always necessary to go through all six phases one by one; rather these may be of different length and may overlap as required,[32] but at each phase, a NAC decision is required to authorise a response.

Another pillar of NATO's crisis response is civil emergency planning that focuses on dealing with consequences of conflicts and disasters. The advice and assistance provided by the civilian experts are always demand-driven. The Euro-Atlantic Disaster Response Coordination Centre is set up to collect requests for assistance and to facilitate the coordination of responses by Allies and partners. In cases when the requestor is not a NATO member or NATO partner country, or when collective Allied military resources are used, the decision to provide assistance to civil authorities must be made by the NAC. Such NAC-decisions have been required twice for providing humanitarian relief to Pakistan: in the aftermath of a massive earthquake in 2005 and following floods some years later. NATO has developed a set of complementary processes to manage crisis and emergencies – the Crisis Management Process, the NATO Intelligence and Warning System, NATO's Operational Planning Process and NATO Civil Emergency Planning Crisis Management Arrangements – that all need to function with synergy.

NATO's history of crisis response operations outside of the realm of collective self-defence (so-called non-Article 5 situations) is mainly about engagements in non-NATO nations with the aim of preventing conflicts and violence from spreading further afield and destabilising regions (e.g., peacekeeping operations in Bosnia and Herzegovina, and Kosovo). NATO has also used deterrent capabilities for conflict prevention and de-escalation by the deployment of operational forces. NATO deployed Patriot missile batteries to protect Turkish borders in 1991, 2003 and 2012, after Article 4 consultations. The Georgia-Russia crisis and the 2007 cyber attacks against Estonia have so far been the only cases where NATO has deployed cyber defence expertise.

NATO's Strategic Concept[33] of 2010 states that NATO has the responsibility 'to deter and defend against any threat of aggression and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a

31 Operations Policy Committee, the Political and Partnerships Committee, the Military Committee and the Civil Emergency Planning Committee.

32 For a complete overview of the NATO Crisis Management Process, including the description of phases, see http://www.nato.int/cps/en/SID-D631C1DB-5F6EB742/natolive/official_texts_75565.htm?selectedLocale=en.

33 Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.

whole' emphasising that cyber attacks 'can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability.'[34] As NATO Secretary General Anders Fogh Rasmussen put it: 'there simply can be no true security without cyber security.'[35] To address these security concerns, the Alliance would 'develop further its ability to prevent, detect, defend against and recover from cyber-attack, including […] better integrating NATO cyber awareness, warning and response with member nations.'[36] It is not yet clear what role the Allies exactly envisage NATO to have in order to assist them in non-Article 5 situations.

NATO's civil emergency planning and protection community's role during a cyber crisis is still to be agreed upon and clarified. Following the tasking received from the Strasbourg/Kehl Summit in April 2009, NATO has established a database of national civil emergency experts specialised in the political, reconstruction, stabilisation and media fields, being 'on-call' for stabilisation and reconstruction operations. This program, called COMPASS (Comprehensive Approach Specialist Support Database) does not currently include any cyber experts. There is another roster of civil emergency experts under the Civil Emergency Planning Committee (CEPC), which includes cyber expertise under one of its four technical Planning Groups – the Industrial Resources and Communications Services Group. These experts from both government and industry are provided by nations for three-year periods, during which they should participate in training and be at readiness to respond to requests for assistance in accordance with specific procedures under the Civil Emergency Planning Crisis Management Arrangements. The Civil Emergency Planning Rapid Reaction Team (CEP RRT) is at 24-hours readiness to be deployed to assess the crisis situation and civilian assistance requirements. The first and so far the only example of a deployment of cyber experts in accordance with the CEP RRT procedures happened in August 2008 as a result of the crisis in Georgia.

There has also been some discussion in NATO on using a 'smart defence' approach to cyber crisis management. Smart defence is a concept developed in 2010-2011 with the aim of meeting new security challenges by optimising the defensive capabilities of the Alliance in times of shrinking defence budgets. Smart cyber crisis management would encourage Allies to pool resources – personnel and technical – to assist other Allies and NATO under cyber attacks. Such pools could also be of assistance in pre-crisis environment, by sharing skills and knowledge to assist Allies in harmonising their national cyber defence preparedness capabilities.

34 NATO Strategic Concept 2010.

35 NATO News, January 2011.

36 NATO Strategic Concept 2010.

Alliance consultation and reaction mechanisms have been tested twice: during the 2007 cyber attacks against Estonia, when NATO sent an expert to Tallinn to observe and assist, and the 2008 conflict between Georgia and Russia, when Georgia received assistance through the Civil Emergency Planning Crisis Management Arrangements. Since then, NATO has adopted a cyber defence policy, establishing the Cyber Defence Management Board to coordinate cyber defence activities throughout NATO bodies and establishing a concept for Rapid Reaction Teams (RRT) to be made available in the event of a cyber crisis. NATO has signed cyber defence Memoranda of Understanding with the majority of Allies, defining information exchange and early warning arrangements, and mechanisms for getting assistance in times of crisis. There is an important paradox, however, in NATO's main mission being the defence of its own networks and Allies requesting assistance. It would probably be difficult to find consensus on the deployment of NATO RRTs to assist Allies if there is a chance that NATO networks may be hit as well. It is clear that responding to cyber attacks requires a high level of coordination and flexibility both from NATO and the Allies.

NATO's response to non-Article 5 crises that involve a cyber component is not yet well defined and regulated, because there appears to be no consensus on to what degree national responsibilities for cyber defence and security should be transferred to NATO. The lowest common denominator among the Allies is the agreement that NATO's primary cyber defence task is defending its own networks. While cyber defence of the Allies is and will likely remain a national responsibility, it is clear that in times of crisis affecting Allies, NATO's cyber defence does not stop at the defence of its own networks but involves some sort of coordinated response, depending on circumstances. The ambiguity of crisis response and coordination mechanism might serve as a deterrent, or even encourage the less-advanced nations to invest in the development of their national cyber defence capabilities. However, the lack of determination may also weaken NATO's image and credibility as a strategic actor in cyber defence. NATO's constructive ambiguity about cyber defence may also be seen as a reflection of unconstructive political disagreements on when and how NATO should be mandated to react. Consequently, instead of deterring attackers, this lack of clear, unified rhetoric might instead make the adversary favour cyber operations over other forms of military or non-military attacks, the responses to which NATO has planned and exercised for decades.

It is clear that agreeing on a set of principal crisis management measures and procedures and testing them routinely in multinational exercises would contribute to national policy processes and the adoption of cyber emergency measures, where these are not yet in place or are inconsistent. NATO has organised the annual Computer Emergency Response Team (CERT) level cyber defence exercises 'Cyber Coalition' since 2009 to establish procedural clarity and familiarity with institutional settings responsible for cyber defence in different nations. Notably, and despite the usual political difficulties regarding cooperation with the EU, NATO has been able to invite the EU as an

observer to the 'Cyber Coalition' exercise. NATO has also integrated cyber scenarios in its annual 'NATO Crisis Management Exercise' (CMX). Contacts and best practices shared through these technical and strategic level exercises can be critical in real crisis situations.

When looking at NATO's current cyber defence architecture, we see a multitude of actors in a spider-web of interlinkages with sometimes parallel competences, limited horizontal cooperation and unclear lines of command and subordination. Perhaps it is time that NATO starts streamlining its structures and processes in order to produce the necessary determination and agility to keep up with this evolving challenge. It is certain that NATO needs to improve coordination between its internal bodies and with the individual Allies in order to prevent redundancy and for the improvement of crisis response procedures. By having clear and concise crisis management procedures in place and tested (on technical, operational and strategic levels), NATO would avoid a situation where a collective response is delayed because of conceptual divergences.

4.2 European Union

The EU has been active in two substantially overlapping cyber security areas – measures to combat cyber crime and critical infrastructure protection – playing an important role in setting and discussing norms and resilience measures to support member states. The EU Internal Security Strategy, adopted in 2010, outlined the need to raise the level of cyber security for all EU citizens and businesses as one of its objectives. This included the creation of a CERT network (CERT-EU) including all EU institutions by 2012, establishment of the European Cybercrime Centre, and the launch of the European Information Sharing and Alert System by 2013. However, in terms of technical, legal, organisational and political cyber defence measures, there are still significant gaps between individual member states in the EU. Fragmentation, stove-piping, inter-agency battles and lack of strategic oversight of the different EU institutions and agencies has hindered progress in cyber security efforts within the EU.

The recently adopted European Cyber Security Strategy is the first attempt to co-ordinate cyber security related activities across a range of policy domains in the EU. The strategy focuses on improving the resilience and capacity of EU member states, fostering cooperation against cyber crime, addressing and developing structures and capabilities for EU cyber defence, and formulating a policy on working towards closing the digital divide and helping cyber security capacity building outside the EU. The European External Action Service will continue its efforts to strengthen dialogue with China and India. A joint EU-US Working Group on Cyber Security and Cyber Crime, created in 2010, needs to be beefed up as well. The strategy will require, via enabling legislation (Network and Information Security Directive), that each EU member state should possess a well-functioning national CERT and a competent national authority responsible for the overall management and coordination of network and information

security. These authorities would be tasked to collect incident reports by companies and should have plans prepared for dealing with major incidents. ENISA was granted a new seven-year mandate in 2013 with an expanded set of regulatory duties, including supporting the development of EU standards for risk management and contributing to the prevention, detection and response to cross-border cyber threats. With it, the agency is expected to play a large role in the implementation of the EU Cyber Security Strategy. The Strategy also steps up the efforts to encompass cyber into EU's common defence, security and foreign policy calling for concepts, structures and capabilities for cyber defence at the EU level.

The Strategy devotes surprisingly little attention to crisis management. EU actions in case of major cyber incidents or attacks are not even listed among the five strategic priorities,[37] despite the fact that three years earlier the Internal Security Strategy listed enhancing Europe's resilience to crisis and disasters as one of the EU's core objectives. In recent years, different coordination mechanisms for interactions between the EU institutions and affected member states in crisis management have been established, and under the EU Solidarity Clause in the *Treaty on the Functioning of the European Union*, the EU and its member states have an obligation to assist one another in case of a terrorist attack or a natural or man-made disaster.[38] But when it comes to responses to cyber crisis, the EU has not been able to match the rhetoric with resources and concrete actions. Sharing and coordination within EU institutions and with and between member states, as well as with outside partners, are still insufficient. ENISA has conducted two cyber exercises – 'Cyber Europe' in 2010, and in 2012 also involving the US – but neither paid appropriate attention to the EU institutional-level crisis management role and ability. The focus of these exercises has been on organisational preparedness at the state level and the efficiency of inter-state cooperation during large scale incidents involving national civilian critical infrastructure. In that respect, 'Cyber Europe' is a useful awareness exercise that helps to test and improve national crisis management procedures, but has less value in fostering the development of pan-European crisis management arrangements. The exercise also engaged the private sector in national teams but it has never engaged NATO.

It should not come as a surprise that the European Cyber Security Strategy is very thin on forward-looking cooperation with NATO. This is an unfortunate development indicating that no serious progress in EU-NATO practical cooperation can be envisaged in the foreseeable future. Yet, EU and NATO should complement and not duplicate each other, as they have a large shared membership and common values. As with other aspects

37 Achieving cyber resilience; Drastically reducing cyber crime; Developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy; Develop industrial and technological resources for cyber security; and Establish a coherent international cyberspace policy for the European Union and promote EU core values.

38 Treaty on the Functioning of the European Union, 2010, Art 222.

of crisis management and civil protection, there is a significant overlap of roles between NATO and the EU. While NATO has a mandate of international crisis management, it cannot contribute beyond the strategic aspects of national security, such as national critical infrastructure resilience building or other issues pertinent to civilian cyber capabilities. The EU on the other hand is unique in its capacity to bring a comprehensive variety of different instruments – civilian and military crisis management capabilities, legislative powers, and resources available for assisting the capacity building in less advanced nations. This is a tool-set that neither NATO nor any other international organisation can compete with. Therefore, the EU should be best placed to take the lead in fostering cooperation with NATO as an integral actor in this comprehensive framework. In addition to duplicating effort and wasting resources, such confrontation creates a lot of confusion for member states. For example, to which organisation would a state that belongs both to NATO and the EU turn to in case of a cyber crisis, since both seem to have crisis management mandate and procedures in place?

As a first step, the inter-institutional battles and disunity between the EU directorates will need to be managed in order to develop a robust action plan for the implementation of the Cyber Security Strategy. After that, perhaps it would be easier to take the second step in the direction of rapprochement with NATO.

4.3 Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) is a regional intergovernmental organisation covering most of the northern hemisphere and focusing on high-level security related dialogue combining the politico-military, economic, environmental, and human dimensions. The mandate of the world's largest regional security organisation includes topics such as early warning, conflict prevention, crisis management, post conflict rehabilitation and the promotion of human rights and fundamental freedoms. One of the OSCE's greatest contributions to international security is undoubtedly its transparency and confidence building measures. The 'Vienna Document'[39] and the *Treaty on Conventional Armed Forces in Europe*, (CFE Treaty)[40] are the definite highlights of the organisation's 40-year history.

Since 2005, OSCE has also been engaged in cyber security matters, such as combating cyber crime and discussing cyber terrorism issues. Several conferences, workshops and best practices manuals on these topics, for example the 'Good Practices Guide on Critical Energy Infrastructure Protection'[41], have fostered multilateral exchanges and provided food for thought in outlining suggestions for OSCE's possible future role in

39 The Vienna Document 1999 of the Negotiations on Confidence- and Security-Building Measures (FSC. DOC/1/99), available at: http://www.osce.org/fsc/41276.

40 Text of the Treaty available at the OSCE Documents Library: http://www.osce.org/library/14087.

41 'Good Practices Guide on Non-nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace'.

advancing cyber security. In 2008, several high-level meetings were held, and, in May 2011, a conference was conducted on a 'Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role.' It became apparent that the OSCE member states seem to agree that a lack of shared understanding regarding the norms of governing states' behaviour in cyberspace could cause misperceptions, promoting escalation and impeding crisis management in the event of major cyber events. Therefore, the OSCE's focus on cyber security became the transparency and confidence building angle. At its 909th Plenary Meeting in April 2012, the OSCE Permanent Council approved a decision on development of confidence building measures (CBMs) to reduce the risks of conflict stemming from the use of ICTs, establishing an Informal Working Group (IWG) 'to elaborate a set of draft CBMs to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.'[42] The Council was hopeful that the working group could elaborate and propose a set of CBMs to be adopted in 2012, but that estimation was very much premature. The Chairman of the IWG presented a draft based on over 50 proposals submitted by participating states. They included several CBMs and stability measures, and co-operative methods of crisis prevention and resolution to be used in the event of 'discrete disruptive activities of non-state actors.'[43] However, the 2012 Ministerial Council in Dublin was unable to find consensus to adopt the draft. The IWG continued to meet throughout 2013 with an aim of finding a consensus for the 20th Ministerial Council meeting to be held in December in Kiev.

The results of the IWG meetings are much anticipated by optimists, as finding consensus on cyber CBMs would signify an important breakthrough in the political deadlock surrounding the East-West dichotomy and help the OSCE to re-establish itself as a serious forum for security debates again. Critics complain of the OSCE's lack of relevance and visibility as a security organisation, and absence of focus. The CFE Treaty has been suspended by Russia, the Astana Summit in 2010 failed to produce a joint action plan and nations have not been able to agree on final statements of several ministerial meetings. It remains to be seen if OSCE will manage to gain in relevance on cyber security. It took a decade for the UN First Committee and three UN GGEs to produce a meaningful joint report on ICT, and there is little reason to believe (considering that the political divisions are similar in both organisations) that the OSCE could succeed much faster.

4.4 Collective Security Treaty Organization

CSTO is a regional security organisation currently uniting six former Soviet Union republics – Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan

42 OSCE, PC.DEC/1039, 2013.

43 OSCE PA, 2013.

(Uzbekistan withdrew in 2012). The CSTO's main mission is collective defence – it has collective air defence capability and Collective Rapid Reaction Forces (*Kollektivnyye Sily Operativnogo Reagirovaniya* – KSOR). The ability of KSOR to react in crisis situations was tested in June 2010 when inter-ethnic violence erupted in southern Kyrgyzstan, risking destabilisation of the whole region. Surprisingly, the CSTO refused to act in response to an assistance request from the interim Kyrgyz government, referring to its strict principle of non-intervention in members' internal affairs. That led to perceptions of the ineffectiveness of the CSTO as a serious actor in regional crisis management. The decision not to interfere was allegedly caused by the lack of a legal mandate to react to internal crises, but there were other political considerations involved. None of the CSTO members seemed to be convinced about the need to take military action. Still, the Kyrgyz crisis made the member states amend the charter of the CSTO to permit intervention in any similar crisis in the future.

The organisation also puts great emphasis on collaborative solutions in cyber security. The CSTO has a 'Program of joint actions to create a system of information security of the CSTO Member States.'[44] One of CSTOs three main joint operations, 'Proksi', is dedicated to fighting cyber crime,[45] and is conducted by the intelligence organisations of the member states. According to CSTO Secretary General, Nikolai Boryduzha, CSTO is 'working on practical activities to ensure information security,'[46] and Operation 'Proksi' is, according to him, aimed at extremists and political provocateurs who 'disseminate information that causes political damage to state and allied interests,'[47] in addition to drug dealers and terrorists. The CSTO recently set up an Association for the Analysis of Informational and Analytical Structures that, according to CSTO Secretary General, was established 'to provide analysis on risks and threats faced by CSTO member states, and to develop pre-emptive measures to keep these threats at bay.'[48]

Sometimes this organisation is described as a 'counter-block' to NATO. While all of its members have partnership arrangements with NATO, it is implied that the CSTO members place far greater emphasis on the organisation than on their cooperation with NATO,[49] and there is no formal relationship established between NATO and the CSTO. The most important difference between these 'counter-blocks' is that, unlike NATO, CSTO seems to have no global crisis management ambitions and does not seek to take part in operations outside the borders of its member countries.

44 McDermott, 2012.

45 CSTO.

46 The other two are 'Kanal,' (anti-drug trafficking) and 'Nelegal' (stopping illegal immigration).

47 Mshvidobadze, 2012.

48 *Ibid*.

49 Chernenko, 2012.

4.5 Shanghai Cooperation Organisation

SCO is another regional security organisation involving Russia and most Central Asian states, but also China. Information security has a prominent place in this organisation. In 2009, the organisation adopted an *Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security*.[50] The agreement defines the basic philosophy and principles that these nations share on information security, and according to some observers this joint statement serves as a comprehensive regional cyber security strategy for Central Asia. One of the most significant aspects of this agreement is a list of terms and concepts, something that Russia has tried to push for in the UN since 1998.[51]

The most prominent initiative on cyber security by the SCO is probably the proposal of the *International Code of Conduct for Information Security* signed by four SCO members, based on the principles introduced in the 2009 agreement on information security. The proposal was submitted to the UN Secretary General in September 2011, interestingly coinciding with the aftermath of the Arab spring. The purpose of this initiative was 'to identify the rights and responsibilities of States in information space, [...] and enhance their cooperation in addressing the common threats and challenges in information space [...].'[52] The subscribing state would agree 'not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, and pose threats to international peace and security or to proliferate information weapons and related technologies.'[53]

SCO, or rather the Russia-China partnership, can be viewed as one of the two centres of gravity in the philosophical and political debates between the two blocks of cyber *versus* information security in the UN. Beyond that, SCO can be seen as having a regional confidence-building role, as it has invested in agreeing on joint terminology and principles that should contribute to misperception management in crisis situations. It is nevertheless difficult to see any practical cooperation refined down to specific projects behind the high-level declaratory statements.

4.6 Organization of American States

The OAS has introduced several initiatives to strengthen cyber security related cooperation between the American states. In 2004, the member states approved 'The Inter-American Strategy to Combat Threats to Cyber Security,'[54] and started to develop different cooperation and capacity building mechanisms, most notable being the effort

50 McDermott, 2012.

51 CIS-Legislation.COM.

52 Baseley-Walker, 2011: 36.

53 UNGA, A/66/359, 2011.

54 *Ibid*.

to foster establishment of Computer Security Incident Response Teams (CSIRTs) in each country and to create a hemispheric 'watch and warning network', providing guidance and support to the national CSIRT teams. The organisation also aims to support the development of National Cyber Security Strategies and promote general awareness of cyber security.[55] OAS has also invested in creating a practical training environment, a Mobile Simulation Laboratory, designed to train cyber security incident-response personnel in member states.

4.7 The Association of South East Asian Nations and ASEAN Regional Forum

ASEAN hosts a Regional Forum (ARF) created to foster political and security related dialogue, consultations and cooperation in the Asia–Pacific region. The forum has hosted workshops on confidence building in cyberspace and on incident response, and has pledged assistance to build capacity in less developed ARF states. At the 20th ASF meeting in 2013, ARF ministers reviewed the progress of the ARF work plan related to cyber security developed – when the 'Statement on Cooperation in Ensuring Cyber Security' was adopted in 2012 – to reduce the risk of 'misperception, escalation and conflict.'[56] Ministers also reaffirmed the importance of intensifying cooperation, including through information-sharing and capacity-building, and agreed on the formation of a 'Seminar of Experts on the development of Cyber CBMs' in ARF.[57]

Calls for regional cooperation in defending the common cyberspace have been highlighted also in the ASEAN ICT Masterplan 2015. The plan envisages the establishment of common minimum standards for network security to ensure a high level of preparedness and integrity of networks across ASEAN, a network security 'health screening' programme, the development of best practice models for business continuity and disaster recovery, and the establishment of the ASEAN Network Security Action Council to promote CERT cooperation and sharing of expertise.[58] In September 2013, marking the 40th anniversary of the Japan-ASEAN Friendship and Cooperation, the 10 ASEAN member states and Japan gathered in Tokyo for a Ministerial Policy Meeting on Cyber Security Cooperation. The ministers issued a statement pledging cooperation between relevant agencies in response to cyber attacks through initiatives such as Internet Traffic Monitoring Data Sharing (TSUBAME) Project[59] and PRACTICE, a collaboration for sharing of observational data about the

55 Comprehensive Inter-American Strategy to Combat Threats to Cyber Security: a Multidimensional and Multidisciplinary Approach to Creating a Culture of Cyber Security (AG/RES. 2004 (XXXIV-O/04)), text available at: http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

56 OAS, 'Cyber security program'.

57 Ministry of Foreign Affairs of Japan, 2012.

58 ARF Chairman's Statement, 2013.

59 ASEAN ICT Masterplan 2015.

analysis and prediction of cyber attacks in order to facilitate proactive response to cross-border cyber attacks.[60] The ministers also stressed the importance of capacity building and awareness initiatives, and of establishing a mechanism for quick response to cyber incidents, including practicing such cooperation through joint exercises.[61] Japan has been previously cooperating bilaterally on data sharing with Indonesia, Thailand and Malaysia. China is also stepping up its cyber security related dialogue with ASEAN. At the ARF meeting in Beijing in September 2013, participants spoke about the importance of cooperation, best practices sharing, and professional and educational exchanges in cyber security.[62]

Secure cyberspace is critical for ASEAN's vigorous economies, against the backdrop of regional interstate competition and potential conflict. The region lacks cohesion and in many cases there are insufficient levels of trust between the countries to act together. Asia lacks strong multilateral institutions and is therefore a sphere of strategic competition in cyberspace, involving espionage and cyber attacks.[63]

4.8 The African Union

The Peace and Security Council of the African Union (AU) is a 'collective security and early-warning arrangement to facilitate timely and efficient response to conflict and crisis situations in Africa.'[64] Its mandate ranges from providing assistance in the provision of humanitarian aid to military intervention. In 2013, the AU Commission and the UN Economic Commission for Africa jointly prepared a draft *Convention on the Confidence and Security in Cyberspace*[65] seeking to harmonise African cyber legislations on data protection and cyber crime. The Convention also promotes cyber security through encouraging the establishment of national CERTs and regional CSIRTs to reduce institutional gaps in the events of crisis.[66] The draft Convention calls for adoption of national cyber security policies and necessary legislative measures against cyber crime, and security and management of national critical infrastructure.[67] The draft has gone through a rigorous review in a series of sub-regional meetings, and was endorsed by the AU ministers in charge of information and communication technologies in September 2012. It is expected to be ratified by AU member states in 2014.

60 Common traffic monitoring system shared among CSIRTs in Asia Pacific region to observe suspicious scanning activities.

61 Ministry of Internal Affairs and Communications of Japan, 2013a.

62 Ministry of Internal Affairs and Communications of Japan, 2013.

63 Hou, 2013.

64 Lewis, 2013.

65 African Union, 2002.

66 African Union, Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.

67 Yankey, 2013.

The AU's practical capability in conflict management is undermined by the lack of financial and human resources and a 'persistent capabilities-expectations gap, falling well short of the ambitious vision and rhetoric contained in its founding documents.'[68] Whether the vague and aspirational statements of AU ministers will actually help to develop new norms and frameworks and commit to the next steps remains to be seen.

5. Informal Multilateral Organisations

5.1 G8/G20

G8 is an informal forum for Heads of States and Governments and their finance and foreign ministers to discuss pressing international issues concerning crisis management, international security, the global economy, energy, and terrorism. Because of its small and static membership, it is seen by many uninvited nations as a rather elitist and arbitrary grouping that excludes emerging powers from key talks concerning global security. As an informal grouping, participating states have little influence to assure compliance with commitments other than reputational harm. On the other hand, its small size enables quick and efficient decisions in conflict resolution. G8 *ad hoc* meetings could be a good example of an efficient escalation tool. The G8 Summits give world leaders an opportunity for candid and unscripted conversations and potentially provide breakthroughs in solving urgent global problems.

The leaders of another informal grouping – the G20 – declared at their Summit in Pittsburgh in 2009 that this forum and not the G8 was the 'premier forum for international economic cooperation.'[69] Indeed, the G20 provides a wider forum, a venue where established and emerging powers can work together, and some have started to describe the G20 as the 'steering committee' for global governance in general. However, there are several issues that dilute that dream. While membership of the club of the invited 20 empowers the sense of elitist political power and probably gives strong incentive to produce efficient and relevant decisions, it may also generate in some nations an understanding of their own exceptionalism, enforcing national red lines and thus raising difficulties in reaching consensus and taking collective action.

Nevertheless, the 'G-s' have the potential to grow not only in membership but also in agenda. While the G8/G20 Summits revolve around political leaders and seem to some critics as mere high-level information sharing venues, they also provide a venue for trans-governmental networks and regular and *ad hoc* task forces and working groups, which foster working-level connections and sharing of best practices.

68 AU, 'Cyber Security'.

69 Williams, 2011: 1.

As a whole, the 'G-s' have a solid record of building commitments and subsequent implementation of collective decisions.[70] Despite the concerns of representativeness and legitimacy, the 'G-settings' have the ability to present a viable supplement to formal permanent mechanisms, such as the UN institutions that have many times been politically deadlocked and unable to find consensus on collective action, and it is probably just a matter of time before the 'G-s' start discussing cyber security and the pressing issues around cyber crisis management.

5.2 BRICS

Representing around 40 per cent of the world's population and a quarter of its economic output, BRIC (an acronym referring to Brazil, Russia, India and China, and now inducing an 'S' for South Africa) emerged as a term a decade ago to describe a group of countries growing in importance and desiring to set the agenda for global politics. Although its main focus is to coordinate discourse on global economics and finance, the annual BRICS Summits and inter-agency meetings have also provided a forum to discuss broader issues, including climate change, threats of terrorism and urgent matters of international security. However, their ability to show unified political force has been limited. The Summits' final communiques tend to be vague and avoiding real joint action on matters of global concern.[71]

Although the 'new BRIC' – the MIST[72] – is far from being a cohesive group capable of or desiring to develop similar standing in international politics as BRICS, there can be other collaboration clusters of states emerging in what Richard Haass describes as a 'messy era of multilateralism.'[73]

6. Formal Networks of CERTs

The Forum of Incident Response and Security Teams (FIRST) is an international union of CERTs, bringing together about 200 members from government, military, industry, and academia to provide a mechanism for trusted information exchange, coordination of incident response, and sharing of tools and best practices. By involving the private sector, FIRST aims to be a global public-private partnership platform for sharing knowledge otherwise difficult to access. FIRST is an effective trust-building mechanism at a working level, uniting practitioners, sometimes empowered stakeholders who represent each country's interests. FIRST also accredits CERTs worldwide.

70 OECD, 2009.

71 Alexandroff, 2010: 6.

72 An acronym referring to the economies of Mexico, Indonesia, South-Korea and Turkey, invented by Goldman Sachs analyst Jim O'Neill, also the creator of the term BRIC back in 2001.

73 Haass, 2010.

FIRST is not the only international network of CERTs. The Trans-European Research and Education Networking Association (TERENA) is another collaboration forum focusing on research networking, and there are many other regional and trans-regional CERT networks which have been established with the aim of sharing information and expertise, and facilitating assistance during large-scale cyber incidents.

7. Conclusions

The organisational architecture of cyber security is rather busy. There is no central international mechanism for cyber crisis management but a large variety of forums with different focuses: incident response at CERT level, civil and military crisis management, transparency and confidence building, and capacity building in less advanced countries.

The international processes for cyber crisis management are relatively weak. Crisis management instruments exist, but most organisations have never needed to test their ability to react in real crisis situations and thus most organisations are still in the learning phase, being reactive rather than proactive, and their capacity to develop new procedures or refine the existing ones is often hindered by political disunity between member states. A major constraint on the development of multinational cyber crisis management arrangements seems to be the lack of trust, coupled with the complexity of stakeholders, institutional inertia, insufficient awareness, and a shortage of resources.

There seems to be a serious gap in inter-organisational coordination of response measures to cyber challenges that leads not only to stove-piping and duplication, but also to inaction, each organisation assuming that the other is taking the lead. These geopolitical schisms between countries hamper inter-organisational cooperation and are not likely to be solved in any time soon.

All international organisations with serious ambitions in cyber security need to vitalise discussions on cyber crisis management measures. For some, the measures are non-existent; for others, they exist but are too cumbersome and confusing. As a minimum, international organisations should develop and promulgate information security standards and disseminate guidelines on best practices. Effective crisis management also needs trusted methods of information exchange, which is more likely to happen in smaller multilateral arrangements and regional organisations. This does not mean that every organisation should have crisis management procedures in place. Depending on the organisation and the given dispute, it may be that no specific procedures are needed, as there are plenty of broader contexts in which to engage in discussions on cyber issues; but even belonging to an organisation of disputing parties means that lines of communication are kept open which helps to avoid miscalculation and the escalation of risks.

Several organisations including NATO and the ITU have taken steps to develop mechanisms of pooling and sharing cyber expertise and infrastructure that are a scarce

resource in most nations. While it definitely is an innovative idea in times of economic constraints, this concept needs a thorough analysis taking into account the issues of availability, burden sharing, national sovereignty and security concerns.

The continuing challenge is the harmonisation of national approaches to crisis management to enable quick and effective responses by national leaders to cyber attacks. It is a matter of bilateral and multilateral diplomacy, information sharing and technical cooperation within or outside existing international institutional frameworks. For international organisations the key to success is not to duplicate efforts already undertaken outside institutional structures.

How the international organisations' approach to cyber crisis evolves and how their international standing develops among other organisations also depends upon their ability to move beyond vague declarative statements. If the declarations are not followed by concrete and sufficiently resourced action plans, their cyber story will be unremarkable. 'Institutional Darwinism' will determine who is fit to address the emerging challenges expeditiously and survive as a player.

The UN, as the foundational framework of international crisis management, reflects the post-World War II balance of powers but it is clear that the 21st century needs different, more flexible settings to address the contemporary geopolitical realities and power shifts. In a multipolar world, countries engage in 'a bewildering array of issue-specific and sometimes transient bodies' seeking to provide the collective effort of decision-making.[74] Cyber crisis management involves coordination and information sharing between governments, industry, academia and civil society, which is a wider and more complex web of interactions than the traditional state-to-state relationship within any existing international organisations.

Since trust is a central issue in cyber crisis management, it seems that the informal 'G-groupings', where leaders engage in straightforward unscripted conversations, could be a favourable multilateral setting for political level cyber crisis management. Participation in these multilateral platforms depends on states' current interests, values and capabilities, which means that these groups are sufficiently homogenous to enable timely response. The 20th century institutions of global governance such as the UN and multiple regional organisations will remain in place, but it seems that the future of cyber crisis management is in more flexible 'G-settings' that give the first political impulse to enable effective crisis management in cooperation with formal treaty-based organisations, as well as with informal professional networks.

Cyber crisis management will definitely become one of the issues of global relevance that determines whether the 21st century world is shaped by confrontation and disorder

74 Patrick, 2013.

or by international cooperation, forging arrangements between global and regional bodies and involving all relevant stakeholders in a concise and non-duplicative fashion.

References

African Union, 'Cyber Security' http://pages.au.int/infosoc/pages/cyber-security, accessed 14 October 2013.

African Union, 2002, *Protocol Relating to the Establishment of the Peace and Security Council of the African Union*, Durban, 9-10 July 2002, http://www.au.int/en/content/protocol-relating-establishment-peace-and-security-council-african-union, accessed 31 October 2013.

African Union, *Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa,* http://au.int/en/cyberlegislation, accessed 31 October 2013.

Alexandroff, A., 'Challenges in Global Governance: Opportunities for G-x Leadership' *Policy Analysis Brief*, The Stanley Foundation, March 2010.

ASEAN Regional Forum, *The Chairman's Statement of the Twentieth ASEAN Regional Forum, Bandar Seri Begawan*, Brunei Darussalam, 2 July 2013, http://aseanregionalforum.asean.org/library/arf-chairmans-statements-and-reports.html, accessed 14 October 2013.

ASEAN, *ICT Masterplan 2015*, ASEAN Publications: Publications Print 2011, http://www.asean.org/resources/publications/asean-publications/item/asean-ict-masterplan-2015, accessed 14 October 2013.

Baseley-Walker, B., 2011, 'Transparency and confidence-building measures in cyberspace: towards norms of behavior' *Disarmament Forum* No. 4, 2011 pp. 31-40.

Becker, T., 2006, *Terrorism and the States: Rethinking the Rules of State Responsibility*, Oxford: Hart Publishing.

Blue, V., 2012, 'Exclusive: ITU "failed," says former policy chief' *CNET News*, 12 December, http://news.cnet.com/8301-1023_3-57558819-93/exclusive-itu-failed-says-former-policy-chief/, accessed 14 October 2013.

Boyle, A., 'Some Reflections on the Relationship of Treaties and Soft Law' *The International and Comparative Law Quarterly* Vol 48, No.4, 1999 pp. 901-913.

Chernenko, Y., 'NATO and the CSTO Approach Security Differently' *Russia Beyond the Headlines*, 4 April 2012, http://rbth.ru/politics/2013/04/04/nato_and_csto_approach_security_differently_24633.html, accessed 14 October 2013.

CIS-Legislation.COM, *The agreement between the governments of state members of the Shanghai organisation of cooperation about cooperation in the field of ensuring the international information security*, 16 June 2009, http://cis-legislation.com/document.fwx?rgn=28340. accessed 14 October 2013.

Council of Europe, *Convention on Cybercrime*, CETS No 185, 23 November 2001.

Crovitz, G., 'America's First Big Digital Defeat' *The Wall Street Journal*, 16 December 2012, http://online.wsj.com/article/SB10001424127887323981504578181533577508260.html, accessed 14 October 2013.

CSTO, *Basic Facts* http://www.odkb.gov.ru/start/index_aengl.htm, accessed 14 October 2013.

ENISA, *Annual Incidents Report 2012*, http://www.enisa.europa.eu/media/press-releases/new-major-incidents-in-2012-report-by-eu-cyber-security-agency-enisa, accessed 14 October 2013.

European Union, 2010, *Consolidated Version of the Treaty on the Functioning of the EU*, 2010/C 83/47, 30 March 2010.

GAO, 2010, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606, 2 July 2010, http://www.gao.gov/products/GAO-10-606, accessed 14 October 2013.

Graham, D., 2010, 'Cyber Threats and the Law of War' *Journal of National Security: Law & Policy*, Vol. 4, No. 87, 2010 pp. 87-102, http://jnslp.com/2010/08/13/cyber-threats-and-the-law-of-war/, accessed 14 October 2013.

Haass, R., 2010, 'The case for messy multilateralism' *The Financial Times*, 5 January.

Hague, W., 2011, *Security and freedom in the cyber age - seeking the rules of the road*, a speech delivered on 4 February 2011 at the Munich Security Conference, https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road, accessed 14 October 2013.

Hou N., 'China to enhance cooperation with ASEAN in cyber security' 11 September 2013, http://english.cntv.cn/program/newsupdate/20130911/103458.shtml, accessed 21 September 2013.

International Telecommunications Union (ITU), 2012, *Final Acts of the World Conference on International Telecommunications*, Dubai 2012, http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf, accessed 14 October 2013.

Klabbers, J. 2009, *An Introduction to International Institutional Law*, Cambridge: Cambridge University Press.

L.S., 2012, 'A digital cold war?' *The Economist* Babbage – Science and technology blog, [online] 14 December 2012, http://www.economist.com/blogs/babbage/2012/12/internet-regulation, accessed 14 October 2013.

Lewis, J., 2013, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia*, Lowy Institute MacArthur Asia Security Project, 07 March 2013, CSIS Publications, http://csis.org/publication/hidden-arena-cyber-competition-and-conflict-indo-pacific-asia, accessed 13 October 2013.

Maurer, T., 2011, 'Cyber Norm Emergence at the United Nations – an Analysis of the Activities at the UN Regarding Cyber-Security' *Discussion Paper 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School*, September 2011.

McDermott, R., 2012, *The Kazakhstan-Russia Axis: Shaping CSTO Transformation*, The Foreign Military Studies Office, http://fmso.leavenworth.army.mil/Collaboration/international/McDermott/CSTO_Transformation-final.pdf, accessed 14 October 2013.

Ministry of Foreign Affairs of Japan, 2012, *ASEAN Regional Forum: Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security*, Phnom Penh, 12 July 2012, http://www.mofa.go.jp/files/000016403.pdf, accessed 31 October 2013.

Ministry of Internal Affairs and Communications of Japan, 2013, *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation*, Tokyo, 13 September 2013, http://www.soumu.go.jp/main_content/000249127.pdf, accessed 14 October 2013.

Ministry of Internal Affairs and Communications of Japan, 2013a, *Collaboration between Japan and Malaysia concerning Proactive Response Against Cyber-attacks Through International Collaborative Exchange ('PRACTICE')*, press release 7 March 2013, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130307_02.html, accessed 14 October 2013.

Mshvidobadze, K., 2012, *Russia's Military Alliance Tackles Cybercrime*, Potomac Institute for Policy Studies, 26 November 2012, http://pipscyberissues.wordpress.com, accessed 13 October 2013.

NATO News, 2011, *Developing NATO's cyber defence policy,* 25 January 2011, http://www.nato.int/cps/en/natolive/news_70049.htm, accessed 14 October 2013.

NATO, 2010, *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation,* Lisbon, 19 November 2010, http://www.nato.int/cps/en/natolive/official_texts_68580.htm#cyber, accessed 14 October 2013.

NATO, *A-Z: Crisis management*, http://www.nato.int/cps/ar/natolive/topics_49192.htm, accessed 14 October 2013.

OAS, 2013, *Cyber security program* www.oas.org/cyber, accessed 14 October 2013.

OECD, 2009, *G20 Leader's Statement, the Pittsburgh Summit*, 24-25 September 2009, http://www.oecd.org/g20/meetings/pittsburgh/.

OSCE, 2013, *Parliamentary Assembly, 1st Committee, Interim Report for the 2013 Winter Meeting, Follow-Up on Recommendations in the OSCE PA's Monaco Declaration,* 2 April 2013, http://www.oscepa.org/component/search/?searchword=Interim%20Report%202013&searchphrase=all, accessed 14 October 2013.

OSCE, 2013a, *Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1039, 26 April 2013.

Pant, H., 2013, 'The BRICS Fallacy' *Washington Quarterly* Vol. 36*,* No. 3, 2013 pp.91-105.

Patrick, S., 2013, 'The Group of Eight Summit: One Pillar of Today's "G-x World"', Council on Foreign Relations Blog *The Internationalist* [online], 13 June 2013, http://blogs.cfr.org/patrick/2013/06/13/the-group-of-eight-summit-one-pillar-of-todays-g-x-world/, accessed 13 October 2013.

Streltsov, A., 2007, 'International information security: description and legal aspects' *Disarmament Forum* 3, pp. 5-13, http://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf, accessed 10 June 2013.

Tikk, E., 2010, 'Global Cybersecurity-Thinking About the Niche for NATO' *SAIS Review,* Vol. 30, No. 2, 2010 pp.105-119.

Touré, H., 2011, *The Quest for Cyberpeace*, ITU and World Federation of Scientists 2011, pp.86–103.

United Nations Counter-Terrorism Implementation Task Force (UN CTITF), 2011, *Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects*, CTITF Working Group Compendium, CTITF Publication Series, New York: United Nations, May 2011.

United Nations General Assembly, 2001, *Combating the criminal misuse of information technologies* A/RES/55/63, 22 January 2001.

United Nations General Assembly, 2002, *Developments in the field of information and telecommunications in the context of international security*, A/RES/56/19, 7 January 2002.

United Nations General Assembly, 2003, *Creation of a global culture of cybersecurity* A/RES/57/239, 31 January 2003.

United Nations General Assembly, 2004, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, A/RES/58/199, 30 January 2004.

United Nations General Assembly, 2010, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201, 30 July 2010.

United Nations General Assembly, 2011, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359, 14 September 2011.

United Nations General Assembly, 2013, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*', A/68/98, 24 June 2013.

United States Department of Defence, 2013, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, http://www.defense.gov/pubs/2013_china_report_final.pdf, accessed 14 October 2013.

UNODA, 2011, Developments in the Field of Information and Telecommunications in the Context of International Security, *Disarmament Study Series 33*, December 2011, http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf, accessed 14 October 2013.

Westlake, A., 2012, 'Japan pushes to form cyber-defense network with other ASEAN countries' *Japan Daily Press* [online] October 2012, http://japandailypress.com/japan-pushes-to-form-cyber-defense-network-with-other-asean-countries-0814818/, accessed 14 October 2013.

Whitney, L., 2013, 'China blames U.S. for most cyberattacks against military Web sites' *CNET News* [online], 28 February 2013, http://news.cnet.com/8301-1009_3-57571811-83/china-blames-u.s-for-most-cyberattacks-against-military-web-sites. accessed 17 October 2013.

Williams, P., 2011, *The African Union's Conflict Management Capabilities: IIGG Working Paper*, October 2011, http://www.cfr.org/regional-security/african-unions-conflict-management-capabilities/p26044?cid=ppc-Google-african_union_paper&gclid=CJaguJityLkCFQMd3godeVoAHg. accessed 10 June 2013.

Yankey, A., 2013, Presentation at the Commonwealth Cybersecurity Forum 2013, 22-26 May 2013, African Union Commission, http://www.cto.int/events/previous-events/cto-past-events-2013/commonwealth-cybersecurity-forum-2013/commonwealth-cybersecurity-forum-2013-presentations/, accessed 10 October 2013.

Zakaria, F., *The Post-American World*, New York: W.W. Norton 2008.

Chris C. Demchak

Economic and Political Coercion and a Rising Cyber Westphalia

In longstanding definitions of interstate coercion, military force and awareness are key components. In a deeply digitised and integrated world, however, these definitions must be adapted. Cyberspace is now a globally shared and critical 'substrate',[1] penetrating widely to more tightly integrated domestic and international systems, both economic and political. Today human struggles travel globally along the connectivity of this substrate, reaching deeply into and across all of the economic and political levels of all digitised and digitising societies. As a result, millions of transactions among well-meaning or predatory actors are forming a highly variable spectrum of 'cybered conflict' between peace and war that will henceforth play a critical role in the outcomes of all societal-level conflicts of the future.[2] Adversaries are able to employ systemic and economically coercive tools with much more modest levels of investment, fewer personal repercussions, and many more opportunities to try again and again.[3] The use of force, which is expensive and very clearly attributable, is thus marginalised to the far end of this spectrum of conflict as inefficient for the purposes of interstate struggles over interests.

In this emergent world, as options and the range of actors in cybered conflict expand dramatically, so do the means of and interest in interstate coercion. Cybered coercion is to traditional coercion as cybered conflict is to traditional kinetic war. Traditional coercion demands preferred behavioural changes from coerced states by using threats clearly stated by coercing states and ultimately based on force. Cybered coercion induces preferred behavioural changes by shaping the reality and perceptions of the nationally essential cybered systems on which the targeted states critically depend. In the globally unfettered cyberspace, states and their proxies, from superpowers to rising,

1 A 'substrate' is much like the concept of the ground on which everything grows. Cyberspace as substrate not only supports and sustains all the systems resting on it, but interpenetrates these critical systems and, critically, continues to grow across societies. One could fairly argue that cyberspace has become, globally, THE shared substrate across societies, unique in that it is a wholly man-made, complex 'socio-technical system', owned and maintained at every point by someone, and contractually allocated for use, profit, and conflict. For a background discussion on underlying socio-technical systems and their unique risks as a substrate, see Mumford (2000) and Comfort et al (2010).

2 The term is the author's own and meant to depict the transitional nature of the idea that cyberspace is new. In the not-distant future, the term cyber will be a redundant addition as everything of critical societal importance will be cybered anyway. See a better discussion in Demchak (2012).

3 Threats in low politics are more powerful than the students of high politics normally accept (Drezner 2003). The globally unfettered cyberspace, however, massively heightens the reach and reduces the entry costs for states to iteratively attempt to engage widely across low politics issues both deceptively and opaquely for some considerable time.

declining, and weak powers, can readily attempt to shape critical perceptions of reality and systems performance or wellbeing in other states (Goldman 2010).

The key caveat is that would-be cybered coercers must maintain both deception and opaqueness throughout their campaigns if they are to be successful; cyber tools built mainly on the deceptive exploitation of flaws in the underlying technologies can be made useless if revealed too early and countered. If identified, the would-be coercers could be punished by equally deceptive retribution campaigns or collective sanctions in other sectors. As a result, economic and other system-shaping efforts tend to be preferred as easier campaign strategies over more obvious political coercion, where it is more difficult for the coercers to maintain opaqueness. Traditional definitions of coercion do not well accommodate the extent to which the global cyberspace substrate has widely and inexpensively distributed means for coercion far beyond the traditional set of major powers and close state neighbours, especially those means which are economic or digitally infrastructural rather than military (Gellner 1992).

This chapter makes four points in addressing the changes to the global system's structure and allocations of power and the emergent cybered coercion induced by a globally unfettered cyberspace. First, the insecure nature of this now globally shared cybered substrate produces a seamless spectrum of transactions among peoples, allowing both wealth and conflict to flow equally well along the same vastly complex networks. Second, cyberspace so tightly couples economic and other societal systems that its insecurities have majorly diminished traditional hindrances to offensive behaviour by states, their proxies, or transnational criminal organisations, making cybered conflict easier and much less risky than the use of force. Third, coercion broadens in its forms and tempo beyond the standard definitions of interstate coercive behaviours, elevating the deceptive, opaque, and relatively low-cost manipulation of economic flows and values of 'low politics' by a wide variety of 'everyman' actors to the level of a major national security issues of 'high politics'.[4]

Fourth, as the global system transitions from its unfettered free-for-all frontier era to a future 'Cyber Westphalia' interstate system,[5] coercion will alter yet again as the state-level cybered protection structures rise across the global substrate. This discussion will integrate the concepts of 'stateness',[6] and economic statecraft with the concepts of systemic resilience and tailored disruption capacities in socio-technical-economic systems as key components of relative national power in a cybered world.

---

4 'High politics' is the classic layer of interstate activities involving war, peace, and sovereignty, whereas 'low politics' has been seen since WWII as economics and other interstate issues not involving military force other than very distantly in the background (Keohane and Nye 1977).

5 The term 'Cyber Westphalia' was first applied by my co-author, Dr. Peter Dombrowski and myself in 2010 in our talks and published in 2011. See Dombrowski and Demchak (2011). Much of the ideas here are those developed from our joint conversations as cyber security scholars thinking systemically over the past few years.

6 See Blanchard, et al. (2008).

1. Cybered Conflict and Systemic Offense without Military Force

The deep penetration of cyberspace as a globally shared substrate underlying the critical systems of most advanced and advancing societies over the past twenty years widely opened the internal resources of these nations to would-be raiders. The connections were built as efficiency measures, meant to advance economic performance and shared knowledge for generativity and, ideally, to improve societal relations and capital development (Zittrain 2006); (Rheingold 1993). Since the 1990s, masses of economic wealth and political power have now become deeply tied to actions in, through, and enabled by the ease, low cost, and ubiquity of cyberspace.

The last twenty years formed a frontier period for this globally shared cyber goldmine (Benkler 2006). The gains have been huge, enabling the unprecedented globalisation of the world's economies (Gartzke and Li 2003). The distribution and redistribution of wealth has also been affected by the ease and vast volume of predation undermining the normal competitive outcomes of putatively liberal and neutrally secured domestic and international markets (Appelbaum and Robinson 2005). The massive significance of what has been taken illegitimately is reflected by the language used by state actors to characterise what has been lost. For example, in 2012, the Bocker Report of the French Senate declared the losses of knowledge, data and money from cyber attacks to be 'pillaging' the economic future of France (Bocker 2012). In the same year, the commander of United States Cyber Command (USCYBERCOM) declared that US losses to attackers led by China were 'the greatest transfer of wealth in human history' (Paganini 2013). In 2012, the Ponemon Institute stated that the top six corporations in the US had alone spent $230 billion dollars in 2010 just on cyber security (Ponemon_ Institute 2012).

States and their proxies now routinely use cyberspace as freely as criminals for acquiring information for leverage and, especially in authoritarian states, for oppression and for transfer of economic advantage.[7] Spies in the form of cyber hackers operate remotely and with minimal personal risk. If the operation is revealed, the software used by spies can be erased rather than having a person tried publicly and then traded or shot. These forms of spies, however, can also produce profit. When ownership is unclear or unguarded, as is the current case with most of cyberspace, states and their proxies can obtain advantages for their national economies by removing valuable information from the servers of competing organisations in other states. Authoritarian states in particular are prone to seeking information with dual use, both to help state strategic leverage and to provide free business intelligence and research and development advantages to

7 See Deibert for an excellent expression of how the errors in code and using commercially easier, type error prone computer languages have produced the downfall of the utopian vision of an open, freely available global web (Deibert 2013).

subsidise their national flagship enterprises' development of both market percentages and bullion (McGregor 2012).

Today the twenty-year frontier free-for-all era of cyberspace is ending, as the victim states have become aware of what was being lost. The international system has moved into a transition era in which groups fight over ownership and control of the wealth and knowledge enabled by cyberspace. Especially at issue is the access to economic wealth and political leverage within and among states, regions, and sectors. Adversaries are using the systems underlying globalisation as tools, arenas, and prizes for control (Gilman, Goldhammer, and Weber 2011). Cyber means intended for societally beneficial purposes are now equally likely to end up in the hands of aggressors, criminals, oppressors, and their proxies (Denning 2010). For example, the online anonymisation service *Tor* has recently been shown to be used mostly not by innocent individuals seeking anonymity for legitimate purposes, but by criminal botnet masters and pornography groups (MIT_ Physics 2013).

1.1 Three Systemic Advantages for Cybered Offense

Cyberspace's open, unfettered, near-free structure encourages this emerging cybered conflict by vastly and systemically diminishing three major obstacles to offense: the scale of organising effective attacks, the proximity required to gather critical intelligence, and the costs of precision in targeting and retargeting broadly. The underlying technical base is designed to deliver packets reliably, not to secure the valuable goods the substrate carries. It is riddled with mistakes in programming and design. These are relatively easy to exploit to gain access deceptively from distance into a wide range of databases, processes, and critical systems essential to governments, huge enterprises, and societies alike. Beyond that, because of the opaqueness of the highly complex technologies to most users, the gullibility of individuals is exploited by attackers, who pose as any number of trusted contacts and induce the unwitting victim to install malicious programs and allow attackers into the now infected computer and its networks (Glenny 2011). With these three advantages, operations are remarkably low cost, low risk, and widely reusable for anyone who has time and internet access, producing a very modern form of democratised predation (Finkle 2010).

1.1.1 Scale in Organising

The first advantage systemically provided by cyberspace's insecure base-layer technologies is that of scale in organising resources for an attack or exploit. Throughout history, would-be attackers or even poachers needed to organise ever larger groups of people in order to cause serious damage to a society-sized defender. That meant that an aggressive state or its proxy would have to spend time and resources gathering people and tools in order to launch an assault. This organising usually took at least seasons, if not years (O'Connell 1989). Now, however, individuals unknown to anyone else can

use the web to organise an attack campaign over hours, days or years with five to five thousand strangers cajoled or bribed via the web into joining the attack.

For example, the attack on PayPal in 2010 by the group Anonymous, in retribution for its refusal to host donation services for WikiLeaks, was led by a core group organised from an online chat room. The key members had never met each other. Nonetheless, they coalesced around their anger and announced the attack via other chat rooms to garner volunteers. They arranged for a distributed denial of service (DDoS) attack using sites designed for the download and installation of software for non-technical enthusiasts to constantly ask for entrance into the server computers. The software allowed the attackers to synchronise their attacks on the commands of a remote central computer and, in some cases, to allow another central computer to automatically control the launch on a private computer in order to keep renewing the attack. Organising the attacks took two days with about 900 volunteers (Olson 2012).

Furthermore, organising for cybered conflict need not involve persuading people, however anonymised by the web. Botnets allow their organisers to employ thousands of infected computers with ease.[8] The relatively unskilled attacker can use the global underground cyber crime market to pay for and thus organise their own small army using the infected computers of tens of thousands, and point the attacks at their desired targets (Goodin 2010a). Throughout history, only super powers or unusually strong neighbours could so readily organise attacking forces to act at their command. For the small Anonymous core group, however, botnets were readily available. In the anti-Paypal campaign, the organisers realised that they needed many more computers to fire and keep firing, but the volunteer pool was insufficient. They then engaged two botnet masters to use their private armies of 75,000 and 50,000 infected machines of innocent computer owners to join into the DDoS attacks. These additional virtual 'zombie troops' were largely responsible for the damaging effects in the attacks, and they were online and firing within four days of the initial efforts to organise (Olson 2012).

1.1.2 Proximity for Intelligence and Reach

The second advantage is how cyberspace massively reduces the need for close 'proximity'. Throughout most of history, attackers needed to be in close proximity to know enough about targets to choose the attack method and timing most likely to prevail. Furthermore, more successful attacking forces used spies to keep updated information on the targets, if possible, in order to make sure that nothing critical to their plans changed, possibly making the attacker's expensive and time-consuming gathering

8 Recent estimates of levels of infection are discouraging. The numbers range from 10-12% in relatively modernised Canada to at least 50% in developing Kenya. See Rafal Rohozinski's talk on October 24, 2013 at http://www.youtube.com/watch?v=ooe4E2bmlQg&feature=youtu.be. See also the 2013 report by the Telecommunication Service Providers of Kenya (TESPOK) industry association at http://usalama.co.ke/reports/Q2-2013/Kenya%20Malware%20Report_Q2-2013.pdf.

of forces more likely to fail (Keegan 2004). Indeed, in ancient Greece, there was a war season – the fall – in large part because that was the only time one could be assured that citizens of another city-state would be willing to come out from behind protective walls to fight to protect their harvests.[9] In other seasons, they might just lock themselves and their goods up behind city walls and refuse to come out, forcing a siege (Hanson 2001). A siege was not only expensive and time-consuming, it also signalled a failure of intelligence gathering, because the attackers had failed to catch defending forces at a vulnerable moment (Russell 1999).

In cybered conflict over unbounded global cyberspace, one need not be proximate to one's targets to be successful in a campaign; distance is enormously distanced as a hindrance. With ease, few costs, and minimal skill, anyone may use the web to gather relatively high quality updated 'signals intelligence' about what method would work best against which target (Deibert 2012). A cybered campaigner generally requires only time, patience, and unfettered access to the global internet, plus a minimal set of computer skills, to hire attack tools from sellers in the global underground cyber crime market (Glenny 2011). Three unemployed Spanish men bought and ran the globally massive Mariposa botnet despite having nearly no computer expertise (Goodin 2010a). Indeed, some botnet resellers now offer warranties, maintenance contracts, and even training, all properly obscured, to the less skilled clients buying or hiring their botnets. They also engage in wars on each other's products (Goodin 2010b); (Buxbaum and Correspondent 2010).

Often what are called social engineering emails or phone calls – i.e., fooling recipients about the true identity of the person requesting information – are preambles to attacks. Rather than having to tediously hack through unknown applications in victim's defences, attackers cajole victims in defending states or institutions into revealing what operating system they are using, among other useful pieces of information. With those key bits of intelligence, the attacker can pick the attack tools most appropriate to that set of applications and operating system.[10]

If knowing more about a target is hard to do without too getting close, software design can be used to compensate by guiding malicious infections in advance around the problematic applications that might be on a target's computer. In this way, distance is

9 Rain was another reason; muddy roads slowed everything to a crawl, including spies who were reporting back what was ahead. Crawling towards a target also meant the target had much more time to prepare, which is always undesirable before battle (Russell 1999).

10 Sometimes one can buy or learn the wrong tools. In 2001, a group of Chinese hackers, angered at the death of the Chinese pilot Wang, announced a US-Chinese hacker war was to occur in early May. The attacks fizzled out in large part because the attackers had learned on open source software like Linux and did not know that most of the servers they would want to attack used the Windows operating systems. That mistake was corrected relatively shortly after that with the massive import of illegal copies of the Windows operating system already cheaply available in Russia. They did score some successes more by accident than informed design (Allen 2003).

still defeated by programming, avoiding having to collect certain kinds of information to use a tool. For example, one of the unique aspects of the Stuxnet worm was that it checked for whether the machine to be infected was running Windows in its 64-bit version or had certain nonstandard kinds of antivirus programs. If those conditions were present, the worm would not infect the machine.[11] Proximity would have been needed to physically interfere with the local owner seeing an alert so the malicious software was designed to exploit proximity where there were Windows 7 in the 32-bit version or Windows XP machines only (Falliere, Murchu, and Chien 2010).

Today malware is often designed as search and then fire-and-forget tools. They are designed for remote use with a mixture of automated and on-call aspects. The first challenge is to ascertain what security and operating systems are installed and to directly fool particular versions from particular firms into accepting the malware as a routine part of otherwise innocent programs. Often the first mission is simply to report back what is installed and then to wait for next set of commands, or to wait for the target to open a particular application, or any other trigger that the designer or botnet owner prefers. In one major case, the Confiker worm, the application replicated easily, rapidly and globally, reaching its peak in 2008, but it did nothing to the infected computers (that we know of) except open a listening port waiting for commands from some as yet still unknown botmaster. Had the master called, millions of computers would have effortlessly released all their data as requested without the owners having any idea of what was lost, where it went, or for what purpose. In the process of discovering the reach and extent of this worm, whole government networks were closed down, ships kept in port, and massive efforts were needed to find and largely (but not completely) remove these quiet, deceptive listening posts. No hands touched the computers, but someone's hands fully meant for those machines to be ready to reply when asked (Lawton 2009). A cybered conflict campaigner can employ all the remote exploitation advantage that cyber crime demonstrates and innovates daily, especially those providing long-term but constant flows of updated information such as the Confiker worm could have done.

1.1.3 Precision of Targeting, Timing, Effects and Replay

The third advantage for the offense in cybered conflict lies in the broad choices in precision for tailoring the timing, tools, and targets of attacks. Throughout history, only superpowers or close peers or dominant neighbours could so easily design, adapt, withdraw, regroup, scatter, or barrage defenders at will with so little investment or risk. Botnets infect millions of unwitting private computers and they can be used for organising barrages on selective targets, for information exfiltration or distortion, but also for experimentation and adaptive behaviours in conflicts and coercion. They have

[11] In the case of a Windows 7 64-bit machine, the concern was that the operating system's embedded security controls would pop up a dialog box asking the local owner to confirm installation and thus reveal the hidden software (Gross 2011).

been found to be actively in residence for years on major networks in government institutions as well as corporate central databases (Mandiant 2013). For what purposes and against what targets the information, system or network access, and controls are used constitute choices left entirely to the aggressor or criminal. In single threads or along multiple avenues of approach, the choices can vary from what is done with that ease of access, whether to distort data, to use the infected computer as a part of an attacking force, to extract copies and use the information to distort markets or to undermine a range of flagship enterprises in a national sector, to publicly humiliate political leaders or privately blackmail them, or to simply sell the extracted data to preferred or highest bidders on the crime or intelligence underground markets (Brenner 2011). The same access can be used to listen, distort, sabotage, destroy, or simply threaten defenders.

Furthermore, installing and lying in residence may be only one set of tools applied to one subset of targets. One may choose to use other tools widely to target whole cities, whole industries, and categories of individuals such as children or military members, or only a few at a time across all these groups, varying the time and duration of any contact. For example, two botmasters engaged by the Anonymous core organisers in the attack on PayPal used their bot armies carefully. They employed a few thousand at a time to keep owners of infected computers from shutting down or rebooting, and also hiding their true numbers in the apparent lists of volunteering IP addresses engaged in the fight. Afterwards, one of the masters became angry and changed the target of his botnet army to the Anonymous chat room itself (Olson 2012). As long as the botmasters can stay personally secure, where their zombie army is targeted is entirely their choice.

Being able to select from a wide range of tools, target differentially and quickly, to the extent desired and with limited costs, and fire or exploit as conditions demand are the operational benefits of the precision advantage. So attractive are these choices that not using all within one's capability could be a sign of a more organised opponent with a higher authority gauging beyond the immediate operational opportunities. For example, the attacks on Estonia in 2007 did not go as far as they could have in the early hours of the first wave, when the Estonian system was reeling from the surprise and not yet able to close down the access points to the nation's central servers. The restraint in those early attacks was also shown to some extent about ten days later when what seems to have been the originally planned mass attack occurred, starting precisely at midnight in Moscow on the date celebrated by Russia as its World War II (WWII) victory day. The evident precision of, at least, the timing, and the breadth of the attacks suggest state-sponsored botmasters engaged in an undeclared campaign using the precision of cybered conflict to make Estonians suffer for the domestic decision to move the statue of a Russian WWII solder (Mansfield-Devine 2012).[12]

[12] Interestingly, Estonia's immediate responses to protect itself had repercussions for its Baltic neighbours in ways that have never been publicly revealed. Furthermore, the attacks waned dramatically after the second and most likely central assault passed after 8 May 2007. Nonetheless, proxies were used to obscure origins and

1.2 Deception and Opaqueness Key to a Cybered Campaign

The three systemic advantages are doubly useful for states or non-state organisations alike as long as their campaigns successfully operate deceptively and opaquely. Both attributes are essential. Deception matters because the tools exploit ignorance of insecurities. Cybered tools are not like tanks which still work even if seen. Once the tool's exploitation method is known, they may not work at all given the corrective responses of the likely targets. Opaqueness is especially important because a revealed aggressor could easily be the victim of equally deceptive and opaque campaigns in return or even attacked preemptively by aggrieved targets, proxies, and allies.

Of the three offense advantages, the near elimination of proximity as a problem in particular helps keep adversaries or their proxies both physically far from victims and far from suspicion. Cybered conflict leaves few 'smoking guns' providing easy associate with a state level actor who might be forced to accept responsibility. The complexity of the technological systems reaching globally, the wide variety of legal prohibitions and surveillance systems across governments and markets, and the sheer volume of other actors, who also attempt to stay unidentified or hindered help both deception and opaqueness. Even relatively active cybered states attempt to maintain both. For example, a 2012 report closely tied extraordinary hacking to a group located in a highly protected building in China (Mandiant 2013). The report was vigorously denied by the Chinese government. Despite extensive additional evidence of such behaviour and even a stated strategy of being willing to use military force in response to unacceptable cyber attacks, the US has not moved to initiate a kinetic military response (Shakarian, Shakarian, and Ruef 2013). Rather, there is ample circumstantial evidence of retributive deceptive and opaque operations by other aggrieved states, none of which are claimed by any of the states involved. Furthermore, many of these punitive or countering operations might well qualify as justified countermeasures in response according to existing ambiguities in international law (Schmitt 2013). Still, no active cybered state is willing to forego the advantages of deception and opaqueness by announcing campaigns, and incurring the wide range of potential blowback costs.[13]

many attacks continued for months, probably as a consequence of the proxies operating independently. Estonia today continues to be something of a national testing ground for aggressors to the East who routinely attempt new techniques in Estonia before refining them to release about half a year later in the rest of Europe and the US. Personal communication with Estonian government cyber security officials as part of a forthcoming case study, August 2012.

13 The number of states with national cyber strategies is rising, but few suggest their nation would actively and publicly engage in such operations in retribution (ENISA 2013). Yet many of the same nations are developing 'active defence', which entails reaching back at cyber aggressors, however vaguely defined.

2. National Power 'Cybered' in State-Level Socio-Technical-Economic System Defence

The nature of power relations across the globe is changing as well. Today the power of a nation has come to rest more and more on cybered capacities. National security is increasingly closely tied to a nation's abilities to systemically secure a wide range of vulnerable public and private sectors critically dependent on a highly insecure cyberspace substrate. National leaders increasingly need to play a key role in ensuring the wider systemic well-being of all deeply cybered major societal processes. The robust cyber power needs to be both resilient to the masses of unskilled 'bad actors' assaulting across societies with botnets and malware, and also able to disrupt the smaller but highly skilled set of organised hackers employed by states or transnational organisations.

For the defender, resilience is key to national power in a cybered world. Means of reducing the flood of easy, low cost attacks must be designed for high volume threats. Aggressor and defender states have already demonstrated a willingness to use the vast armies of cyber criminals as cover to obscure the actions of their own hackers and botnets, if they have the ability to do so. Furthermore, states widely use the innovation in new tools found on the underground cyber crime black market to equip their own highly skilled persistent wicked actors.[14] Since these attackers form the vast majority, the rise of obstacles, especially national borders, is a logical consequence of national needs to reduce the efficacy of these assaults. The gradual rise of national jurisdictions in a future 'Cyber Westphalia' interstate system is already apparent in trends seen from democratic civil societies to those more autocratic nations which would have been interested in having such virtual borders anyways (Demchak and Dombrowski 2011). This will be discussed in the final section.

In addition, and importantly for potential retribution or countermeasures among states, cybered national power for a defender must have a second component aimed at disrupting the highly skilled proxies or actors of other states (Demchak 2012). Disruption needs to be proportional and legal, but able to discern and derail these 'wicked' actors who deftly use camouflage, cover, and the tools of the cyberspace substrate. States may take a 'free ride' on their mass of bad actors undertaking 'patriotic hacking'[15] for objectives including economic extractions for market advantage or intelligence for future political, economic, or even military leverage. However, they actively employ the wicked actors for whom the virtual borders stopping the masses are not effective deterrence. These disruptive capacities will need to change the business model and calculations of efficacy

14 It would be remiss not to mention that virtually all of Stuxnet's successful roaming elements were first innovated by the vast underground cyber crime community. For a detailed discussion of these elements, see the Symantec report from 2010 (Falliere 2010). Also, for a view of how hacker tools are adopted by larger state actors, see Farwell and Rohozinski (2011).

15 This is the term for state tolerance of otherwise illegal hacking as long as the victims are outside the state's geographic borders or those of close allies. See Denning (2010).

and risk that such highly skilled actors use when weighing operational choices (Mallery 2011 (2009)).

A nation's cyber power relative to other states in the future is being built now by the efforts made during this transition era to develop national systemic resilience and forward disruption capacities. It is already difficult to keep up the level of resources needed over the next fifteen to twenty years to anticipate and secure against potentially hundreds of thousands of unidentified bad actors using unknown or unpatched exploits, and to develop the tailored, well skilled, targeted disruption capabilities needed. The open unfettered cyberspace allows for the obscured hollowing out of a nation's economic resources, often over years, and without it seeming to be extensive enough to be dangerous or deliberate enough to require national level responses. Over time, if nothing happens the economic resources of the nation decline, as do the abilities of policy makers to be able to afford to act in defence of all the nation's vulnerable integrated systems. There will be relative winners and losers, from poor to robust, rising and midlevel cyber powers. It is in this context, then, that cybered coercion operates differently on systems and without force.

3. Cybered Coercion: 'Everyman' Shaping of Systems

The standard definitions of interstate coercion vary greatly, but most assume that force and the awareness of the coerced state are present. Just as there are soft and hard power theorists, there are soft and hard coercion theorists and associated definitions.[16] Coercion involving the threat of force is relatively obvious and somewhat difficult to differentiate from the normal exercise of power. Most standard definitions of coercion involve changing the incentives of a state by demonstrating force and the willingness to use it, or by demonstrating the ability to change the benefits received by the state; these are, respectively, hard and soft coercion (Dobbin, Simmons, and Garrett 2007). Farer defines coercion as any means used to influence another state's policies that is not cooperative (Farer 1985). Amongst other authors, however, coercion commonly means known and usually major powers with considerable military force which use political and economic means to demand that other actors change their behaviour. If the coercer state is sufficiently large in traditional power terms, it could coerce by shaping the target state's decision environment such that the actors being coerced perceive themselves to have few alternative options but to change their behaviour as requested.

Even when force is not a major variable, the identity of the major power able to use it is always known in these definitions. Economic coercion is one form of recognised

[16] 'Hard' power is directly associated with overt and direct use of military force or threats, and long associated with the realist school of international relations. See Waltz (1979) for a classic example. 'Soft' power is more associated with using lateral, less direct, and less militarised forms of power demonstrations and tools to achieve national interests. See Nye (2011) for an excellent updated discussion.

coercion in which force is clearly only a background variable; however the coerced state is clearly still aware of the coercer and its demands. Many scholars of international relations define economic coercion as any instance in which the government threatens to interrupt economic relations to force a particular behaviour from another state (Eaton and Engers 1999); (Morgan and Schwebach 1997).[17] When force is not a major variable, political coercion is defined as situations in which the coercing state is known and demands policy changes in the behaviour of another state, either in the domestic or international arena. For example, linking human rights to economic sanctions marginalises force, but clearly demonstrates political demands being made by known entities and punitive economic consequences for noncompliance by the targeted state (Lenway 1988). Thus, in these definitions, even if force is removed to a background contingency and economic systems are the main tools of pressure, the coercer did not hide the origins of the demands.[18]

When the coercer is identified, even when force is not a major variable, coercion can fail in traditional terms if the campaign is exceptionally 'soft' and the behavioural changes too extreme. The coerced political leaders can push back against the coercers by having sufficient 'stateness' to resist the coercion. That is, the targeted nation's leaders have sufficient autonomy, capacity, and legitimacy internal to the nation and relative to the coercer to resist the calls for behaviour change, and to endure or neutralise the consequences of noncompliance if executed (Blanchard, Mansfield, and Ripsman 1999).[19] In these terms, it is not the relative 'hard' power of the state that generally ensures its ability to resist, but rather the defending state's internal resilience and thus ability to withstand or endure the consequences, if they have been able to identify the coercing and thus threatening state against which to organise.

3.1 Cybered Coercion: Forceless, Faceless and Fearless

The difficulty today is that interstate coercion in the cybered world occurs best without force or awareness, much like cybered conflict occurs largely without kinetic exchanges or overt declarations of war. New definitions are needed to accommodate a new form of 'cybered coercion' now available to a wide plethora of actors and proxies, not just to

17 'Coercion includes all concerted application, threatened or actual, of action that commonly causes loss or damage to the persons or possessions of individuals or groups who are aware of both the action and the potential damage.' (Tilly 1992, p.19).

18 The weakest form of this kind of coercion would be labelled in international relations as 'coercive diplomacy'. 'Coercive diplomacy' applies pressure in a manner and magnitude that 'seeks to persuade an opponent to cease aggression rather than bludgeon him into stopping […] just enough force of an appropriate kind to demonstrate resolution and to give credibility to the threat that greater force will be used if necessary.' (Jentleson 2006, p.2).

19 '[…] the political effects of economic signals will depend on a variety of international and domestic political factors, the most important of which is the target state's level of stateness, comprised of three components: autonomy, capacity, and legitimacy. When economic statecraft motivates key domestic coalitions to push for policy change, high stateness enables target state leaders to resist their calls and defy the sender. Conversely, when economic statecraft convinces target leaders that they ought to comply with the sender's demands, high stateness enable them to overcome domestic opposition.' (Blanchard Ripsman 2008. p.371).

major powers or close state neighbours. With the current structure of the open cyberspace substrate and the tools of the global cyber crime market, virtually any state or its proxies now can deceptively and opaquely attempt to shape the behaviours of another state through manipulation of the wellbeing of the cybered systems underpinning the target's society. Such coercion can be economic, but it reaches beyond the traditional changing of incentives to changing the digitally maintained systemic conditions through which incentives are perceived and created. The 'force' of cybered coercion is found in the deceptively altered but seemingly undisturbed, neutral outcomes which the decision makers face, and awareness of who is attempting to coerce is to be avoided throughout campaigns. Under these conditions, leaders of targeted states are unable to use their 'stateness' to respond to coercion explicitly when no state behind the manipulations can be identified. The coerced state may ultimately come to suspect its data, leaders, and markets are being manipulated by a host of cybered means, but would be unable to prove to its own internal stakeholders that these systemic effects are more deliberate than organic, and that collective protective actions are needed in response.

Cybered coercion generally strongly trends towards the manipulation of economic or infrastructural systems rather than the diplomatic means involved in political coercion. The latter is difficult to conceive and implement, as it at least requires that the coercer is identified. Without economic or other means of compulsion, political coercion ultimately rests on reputation or force. As a result of this economic and infrastructural bias, cybered coercion operates more as coercion did before WWII and before scholars of international relations developed the longstanding distinction between high and low politics (and thereby also coercion). The post-WWII neglect of 'economic statecraft' as low politics harms the ability of states to truly understand the nature of economic coercion today (Drezner 2003).[20]

With deception and opaqueness managed during the coercion campaign, the would-be coercer state exploits the systems critical to the targeted state's ever increasing integration between economics and national security. To be successful, coercive campaigns endeavour to arrange for high systemic economic costs to be perceived by targeted state's private as well as public leaders, and to be associated by them with behaviour deemed undesirable by the would-be coercers. The low cost of operations through cyberspace in any case tends to reinforce existing inclinations on the part of national leaders to use economic sanctions or other tools in lieu of military force (Palmer and Morgan 2011). These choices become all the more attractive if the use of tools can be achieved without the coercive state or its leaders publicly identifying themselves,

[20] However, cybered coercion still differs from pre-WWII economic statecraft, because the older versions of coercion were still embedded in notions of war, diplomacy, and state-state threats and posturing that could change the established borders of states. See Doyle (1997) for an excellent discussion of systemic efforts to compel other states.

thereby avoiding any retribution, public posturing in resistance, or collective sanctions by other states.

Just as economic sanctions used by super powers depended on the means more than the precision of the ends, in cybered coercion, the means are easily obtained and can be iteratively or experimentally employed over time in many operations towards ends that can be defined precisely or loosely (Baldwin 1985). If one need only the manipulate background variables of economic analysis to induce desired behaviours, then it is attractive to opaquely experiment across a wide range of campaigns and tools for a considerable time to determine the best methods for achieving those behaviours, especially if the tools can be used deceptively without being discovered and neutralised. Putting force aside, in a cybered world with cybered conflict, would-be coercers and their proxies 'persuade' the systems of the target states rather than their leaders. The operations may use a variety of indirect mechanisms based on societal dependence on cyberspace, from mass effects in the form of political outrage, economic swings, resource declines, safety and security failures, to, if skilled enough, behind-the-scenes widespread data manipulation.

Cybered coercion works today because threats to economic systems traditionally found in low politics often worked without being implemented (Drezner 2003). During the pre-cyber era, states able to manipulate the economic wealth and relative dependence of lesser states were best placed to coerce other states and resist coercion in return from their peer states (Lenway 1988). If resisting coercion by a state in the pre-cybered world required the political 'stateness' identified by Blanchard et al (2008), then today resisting coercion in the cybered world of deeply integrated economic systems requires 'economic stateness' as well; that is, the resilience of whole systems of a state within itself. Today, the successful cybered coercion campaigns economically the resources needed for national stateness and the development of national cybered systemic resilience. Indeed, such a long term cybered coercion campaign may be fairly labelled a 'counter-resilience' campaign. Properly employed, if a successful campaign is occurring, then the target state should not be able to gather sufficient, defining and attributable evidence to demonstrate to their own stakeholders the validity of their accusations against the coercing state, nor to gather sufficient resources and internal support to reinforce resilience policies, institutions, and technologies in defence or for retribution.

It is at the point when target state(s) fully realise their weakened economic circumstances – especially in autonomy and vulnerable internal capacity – that a coercer state may choose to overtly or tacitly 'suggest' state level behaviour changes. If the counter-resilience campaign is mature enough, the targets of the coercion will perceive few economic or political choices but to change their behaviours as desired. In this regard, the coerced state's leaders are likely to be receptive to the other main strategic tools, roughly grouped in the categories of information, capital, and command of technology,

by which more detailed systemic 'suggestions' can be made, especially if made in terms of what the targeted state views as essential life needs being placed at economic risk.[21]

Cybered coercion viewed in theoretical terms is a struggle between whole systems, rather than leaders. As such, understanding its cumulative effects across the wide range of actors and complex systems invites a reframing in terms not associated with standard American international relations. These systemic terms move away from any convenient equilibrium theories to other long wave notions of discontinuities, singularities, attrition, extinction, shifts not along a curve but *in* a curve both up and down, fragility, nonrobust uniqueness, irreproducibility, unrecoverable tipping points, and other terms of complex socio-technical-economic systems analysis (Miller and Page 2007); (Tainter 2006; Walker and Salt 2006).

In this increasingly economically fraught environment, there is no reason to expect that westernised states are less vulnerable to cybered coercion than any other. 'The keys to success are a coercer state strategy that combines carrots and sticks […] against a target state in which domestic political and economic conditions act more as "transmission belts" than "circuit breakers" for the external pressure and persuasion.' (Jentleson 2006). Larger or wealthier states may be less and less able to resist the low politics forms of economic coercion precisely because their private and public leaders do not believe it is possible for their states or their market processes and indicators to be coerced given the hubris and relative autarchy of the Cold War and immediate post-Cold War periods. In 2013, out of concern for the declining British economy, the British Chancellor of the Exchequer George Osborne went to China and essentially publicly invited Chinese information technology (IT) investments to increase in the UK despite several years of strongly growing evidence of massive losses in intellectual property and widespread infection of key economic sectors by hacking groups based in China (Hamill 2013); (USCC 2012). One might argue that cybered coercion resembles a cybered extension of Nye's 'soft power' if it was more deceptively distributed, with obscured proxies carrying hidden electric guns aimed at the target's critical resource systems and set to economically stun, but able to massively disable key sectors if soft power suggestions by a variety of players beyond major powers are rebuffed (Nye Jr 2011).

3.2 Campaign Planning Questions for Coercers

Control of knowledge about the means and origins of a cybered coercive campaign is critical for the coercing state. In particular, planners must ensure that their deception plan for the tools is operationally ensured lest the mechanisms be countered and

[21] I have a long discussion of how the theory of action matches these strategic tools to the key drivers of a remote or unreachable target's decision to act in order to disrupt or delay that decision despite the inability to physically reach them. See Demchak (2011). Interestingly enough, in this case, the coercer would use it not as I intended, but in reverse, against the largely democratic civil societies perennially short of funds.

rendered useless, and that opaqueness in campaign origins is well maintained to avoid resistance or punitive blowback costs.

Today it seems almost banal to note what Sun Tsu said about winning a war without using military force. Yet his guidance to military leaders about strategies also describes in warlike terms much of what a successful cybered coercion campaigner should do in order to never be seen to coerce and yet prevail in attaining the desired behaviours. The modern applicability is clear in the following admonitions, as translated by a senior general of the Chinese People's Liberation Army who is also known as an ultimate insider to both the politics and policies of the Chinese government over four decades:

> All warfare is based on deception. Therefore when capable of attacking, feign incapacity; when active in moving troops, feign inactivity. […] Hold out baits to lure the enemy. Strike the enemy when he is in disorder. […] Avoid the enemy for the time being when he is stronger. […] If he is arrogant, try to encourage his egotism. If the enemy troops are […] united, try to sow dissension among them. Attack the enemy where he is unprepared, and appear where you were not expected. […] To subdue the enemy without fighting is the supreme excellence. Thus, what is of supreme importance in war is to attack the enemy's strategy. Next best is to disrupt his alliances by diplomacy. The next best is to attack his army. And the worst policy is to attack cities. […] Plus, those skilled in war subdue the enemy's army without battle. They capture in the enemy's cities without assaulting them and overthrow his state without protracted operations. The aim is to take all under heaven intact by strategic considerations (Hanzhang 2007).

Putting the essence of these admonitions into modern terms, the following strategic questions must be answered, all of them resting critically on having very timely knowledge in advance:

- What is the behaviour being sought, and how would we (the coercing state) know if it is happening?
- What can we do to make sure the operations adequately deceive onlookers as to how conditions are being altered to induce desired behaviours, and how would we know how well operations are doing before the operations are revealed and countered?
- How can we ensure that we are not blamed for the manipulation, or, if blamed, not forced to accept responsibility internationally?
- How would we know if we are losing control of our opacity and how would we counter the consequences if we do get blamed?

- What are the capacities of the coerced state and its allies to resist the conditions we are manipulating, and how do they routinely ascertain and maintain their economic stateness?

Coercive cybered operations in particular require knowledge of complex social systems, complex economic systems, and largescale complex technological systems, all blended in largescale socio-technical-economic systems designed, used and maintained by humans (Mumford 2000); (Comfort et al. 2010); (Summerton 1994). In that vein, other operational questions to be asked, reassessed, and refreshed continuously include the following (they are adapted from the normal questions of a business or military campaign for a cybered world):

- Timing: to what extent can a revelation of an infection or manipulation be delayed or avoided, how catastrophic is that revelation, and to what extent does it prevent the later reuse or exploitation of tools, targets, techniques, arenas, proxies, or timings, or their application elsewhere?
- Adversary Resilience: to what extent does the target have the resources to scramble an effective technological response in a short period of time with skilled teams, resources, and intelligence, and how can different choices made just prior to or during the operation in applying tools, targets, techniques, arenas, proxies, or timing be manoeuvred to keep target states as long as possible confused, paralysed, distracted, uncoordinated, and ineffective across a wide variety of location, policies, institutions, stakeholders, and applications?
- Other Proxies: to what extent can the insertion of social media misinformation help directly or indirectly to coerce a preferred range of behaviours by a target state and yet obscure the origins of the misperceptions?
- Control over time: to what extent can coercive manipulation operations be coordinated just-in-time or how can they be structured to operate autonomously deceptively if necessary in order to maintain the opacity of state involvement, especially when mediated by less than reliable proxies?
- Opportunities: to what extent can any defensive arrangements in the target state be surprised and overwhelmed by a variety of other short-term and long-term coercive systemic operations which are implanted covertly and can be held in reserve until serendipity provides the opportunity to act, and to what extent need these assets be directly coordinated to avoid misfires and revelations or be automated to act on remote commands without being traced?
- Reserves: to what extent can these efforts to secure the target vulnerabilities be maintained and kept reliable for the longer term in stasis, waiting to be used or reused, and to what extent can one develop and store for the inevitable one-shot use those inherently undeniable tools, targets, techniques, arenas, proxies, or timing preferences until they are best employed?

- Adversary Backup: to what extent does the target state have allies with any of these resources for an effective response to coercive activities, including intelligence and detection technologies and institutions, shared disruptive capacities, and backup arrangements for co-evolved forms of resilience, and can these arrangements be undermined, disturbed, or neutralised in ways favouring the cybered coercive campaign?
- Campaign Backup: what is plan B and a host of backup operations and plans to avoid losing the deception and opaqueness advantages of cybered coercion, and to what extent can recovery in the case of campaign failure be orchestrated into other lateral advantages?

These questions are only exemplary and emphasise heavily the need for asymmetry in knowledge between the coercer and the coerced concerning the truth about what is being attempted. If revealed and widely taken as proven, the coercing state has a much harder task to use the neglected and overlooked avenues of manipulation that were open and when they were not being suspiciously observed.

For a would-be coercer state to lose the advantages of opaqueness with so many deceptive avenues of retribution is, in particular, quite dangerous, depending on what operation is revealed and how widely and deeply losses are perceived. Today, if a major cybered coercion campaign fails and the perpetrator(s) are publicly revealed, given the criticality of economic systems, the adversary is now alerted. That fact elevates the chances that other mechanisms along the spectrum of cybered campaign will be engaged, possibly cumulating through mistake or misperception in cyber-kinetic exchanges. As long as low politics can, through cyberspace, have 'high politics' level of consequences, there are no guarantees that what threatens economic or infrastructural systems anonymously and deceptively through the web does not cascade much further to where conflicting parties rediscover the value of military force. Unfortunately it is currently much too easy and attractive for states to enter into attempts to shape cybered systems and national realities, especially across complex economic systems.

4. Rise of the Cyber Westphalia

As this transition era eventually comes to a close, the unfettered web will be complexly crisscrossed with borders, gateways, filters, dark holes between jurisdictions, national cyber security forces, and a plethora of strategies, only some of which will be coordinated. The relative distributions of national cyber power will be solidifying according to how well each state has developed its own resilience and disruption capacities. The world's states will cluster in groups of robust, midlevel, and poor cyber powers, with the first two more likely to attempt to coerce the third, and the poorer states simply trying to not lose too much in compliance.

The insecurities of the globe's cyberspace are already inducing these changes to the topology of the international system. In this era of the rise of cybered conflict, its forms of coercion, and struggles to allocate and enforce ownership across this substrate, states are acting in ways to increase national security in cyber terms. The result is the emergence of a wide array of national and subnational tools for controlling what the nation's or enterprise's leaders' view as their cyberspace. Filtering, firewalls, encrypted clouds, gateways, and even national laws enabling state monitoring of internet transactions for broad security purposes are rising across democratic states from Sweden to the US (Bambauer 2009). These security-led decisions are creating the building blocks of the future national borders in cyberspace. As national jurisdictions in cyberspace are outlined by these cumulating building blocks, eventually the states of the world create a 'Cyber Westphalia' (Dombrowski and Demchak 2014). In particular, the emergence of cyber security specific agencies and rules on both public and private actors further the development of the notions of what is a national jurisdiction in cyberspace and what is not (Deibert, Palfrey, Rohozinski, and Zittrain 2012).

The presence of cybered borders will also change the conditions for coercion, forcing further adaptations if states desire to change other states' behaviours in the coming era. Coercion may be more difficult to implement due to the increase in difficulty and possible risks of cybered conflict for the lower level actors. The complexity of deception and opaqueness requirements will rise. The relative ease of a Mandiant report in directly tracking high skilled attackers to a specific building in China will vanish. Correspondingly, it may be much harder for a state to persuasively demonstrate this behaviour by another state if the latter has been successful. That is likely to mean future cybered coercion – when successful – is likely to be harder to identify and resist early because it is even more deeply buried than today.

Precisely how the emergent cyber Westphalian system will be structured is unclear, but several of key offensive advantages in cybered conflict will dramatically alter under most conceivable future conditions. First, proximity will once again become a problem for conflicts, coercion, and criminals. The rise of cyber jurisdictions immediately begins to reinstate the security value of distance in cyberspace and diminishes the proximity advantage to the offense. It will be harder to hide in a cyber-bordered state and reach across other bordered states and through encrypted clouds to a target state to acquire the economic and societal intelligence so easily acquired today. Furthermore, it will harder to stay undetected in exfiltrating huge data streams illegally back through all these gateways or cyber-challenging systems without being detected by someone monitoring big data for anomalies.

States with considerable cyber power (in both resilience and disruption) will have the expertise to work around these obstacles, but the vast majority of everyman attackers

will not have those skills. In short, the vast 'noise'[22] afflicting the monitoring systems of today's beleaguered national or commercial cyber defenders is likely to be vastly reduced. It will be more challenging for the highly skilled state sponsored wicked actors, in part because they too must work around, through, or deceive those controls. With the reduction of the vast numbers of inferior skilled actors, their actions will be less camouflaged and more likely to be discernible with ever more accurate cybered hunting and monitoring systems.

Secondly, it will be harder to use the scale advantage to organise 'attacking forces'. Cyber chat rooms and other social media that today transcend all virtual borders will continue to exist, but are unlikely to be so anonymous if those who join must cross jurisdictions to engage in the chat room in order to plan virtual operations. Furthermore, having cyber jurisdictions means that economic transactions are also to be more easily, ubiquitously, and closely monitored for compliance with the laws of the jurisdiction in which they originate, pass, or conclude. It will become more difficult for non-nationals to readily cross monitoring borders to join in organising efforts for cybered campaigns. The potential scale of organising will begin to decline as well, limited increasingly to what is possible largely within one's own cybered borders and subjected more directly to the rules of that government in terms of private communications. The underground will continue, but its activities are likely to become more consistently professionalised, as more skill will be needed to take advantage of looser or weaker cybered jurisdictions more reliably and efficiently; more like drug cartels than the cybered street gangs of today.

Other than further reducing the numbers of low level actors used for cover, this loss in scale only affects the high skilled state-sponsored actors in slowing the underground cyber crime community's rates in developing new tools to be then taken up by the state actors for free. The time and attention of the criminal toolmakers will be diverted from innovative tools to finding ways to undermine the rising variety of national jurisdiction controls just to gain the access and ease that today is virtually free. This means low-skill members of the criminal community will try less often to penetrate beyond many borders illegally, and turn their focus either on their own nation where they are not prevented by borders from acting or on the poorer cyber power states with ineffective virtual borders. Both of those targets and the tools developed for them would be of less interest to state-sponsored actors unless their own home states were peers of the cyber power poor states. In any case, they would have to work on developing their own innovations more unilaterally.

22 'Noise' is the vast volume of hackers, opportunists, and botnets that catalyse widespread calls for national hygiene and a host of other programs just to reduce the load on all kinds of cyber defences. See Clarke and Knake (2009), and Brenner (2011) for discussions of how the volume of small attacks is the most pressing immediate problem of an unfettered cybered world.

Precision remains an advantage, in that one can still opaquely amass and broadcast a variety of tools against a wide and diverse array of targets at once, in barrages or in small groups at one's whim. However, staying opaque across defended cyber jurisdictions will be much harder without the cover of millions of low level actors. Acting with deception over time with complex campaigns will be more difficult as well. The rise of national protections embedded in new border technologies tends to make even formerly easy targets harder to attack. Again the mass of successful low-skill actors are likely to turn inward, reducing the massive flows of attacks and making any campaigns coming across borders with any discernible regularity and precision more likely to be perceived and thus much more risky than today.

In this case, the high-skill actors have the same problem as the low-skill actors in attempting deceptive and opaque mass attacks. The targets can be planned with great precision and skill, but the campaign has to be executed either very slowly at a very low level to maintain deception and opacity, or all at once, thus blowing the reuse of tools but increasing the chances that the one-off nature of the attack will deny any identifying pattern to monitoring systems. A campaign is unlikely to escape some kind of detection if large chunks are executed with any discernible sequence or pattern in origin or method.

The extent to which cybered conflict and coercion continue in the transition era as they each are developing today will also depend on the rules of good state behaviour. How the rules are developed, implemented and enforced, over which states, and thus over which elements of the global and national economic systems, strongly influence the ease of cybered coercion in particular. Patriotic hacking could continue to be tolerated in a state even if other states are finally able to point to the originating state and demand that the behaviour be stopped, as long as the accused state is itself a major cyber power able to resist punitive and likely highly deceptive countering disruptions.

Conversely, if the mechanisms are standardised, the technological detection systems harmonised, the alerting frameworks continuous and efficiently adaptive, and the required responses enforced effectively and communally, the originating state, even if a major cyber power, will have difficulty in continuing to allow such outgoing activity. In the current and future cybered world, being resilient also means in some sense being autarchic in key areas for national survival, most of them economic and infrastructural. To continue to turn a blind eye to these domestic actors hacking outward under these rather ideal circumstances, even a major cyber power would have to also be willing to incur and endure punitive actions by other states.

Cybered coercion becomes more complicated even for relatively robust cyber powers when cyber borders rise. It becomes harder to continue to deny responsibility if campaign actions are revealed by monitored sequences of border crossing captured by collectively compatible and legitimated border technologies which point to the originating state. The state attempting the campaign might be forced to withdraw from other global communal

arenas and would have to have a plan to survive if that was to occur. Or, even if the state now under suspicion has managed to compromise or compel other states to refrain from joining publicly in the communal recriminations and sanctioning, the would-be coercer state still runs the great risk of being the target of multiple coordinated collective or unilateral punitive cyber campaigns that may or may not be overtly declared. These are likely to be rationalised by others as justified punitive actions for poor state behaviour.

In the future, the underlying technological designs and economic flows of cyberspace will change again. The many lists of emerging 'disruptive' technologies offer windows into what is likely to be available for all cybered actors, from coercers to criminals to opportunists to defenders. Recently the McKinsey Group published a list of twelve disruptive technologies which included the rise of big data, widely embedded mobility across the internet of things, and heavily encrypted clouds. Several in particular directly affect the ways in which cyberspace has tightly coupled economics to national security in the current globally unfettered substrate: 3D printing, advanced robotics, autonomous vehicles, and renewable energy (Manyika, Chui, Bughin, Dobbs, Bisson, and Marrs 2013).

With 3D printing and advanced robotics, mass manufacturing can become more efficiently distributed to on-site production facilities catering for and tailored to local needs, thus returning productive forces to the nations that by and large consume the products. That means that mass globalised economic transactions capable of being distorted in cybered ways could be increasingly under only one national or regional jurisdiction with responsibility for assuring security. There is much less likely to be a global demand for exports of a product when each nation could produce it themselves with advanced robotics or 3D printing. Ironically, this process of moving to small scale local industrial production is exactly the process of industrial indigenisation promoted in the 1960s for developing states (De Janvry 1981). In many respects, all nations are developing nations in a deeply cybered world, and many will continue to develop as the Westphalian cybered borders emerge.

The latter two disruptive technologies enhance the renationalisation drivers of the former two. Autonomous movement of goods is more likely to be trusted within than between nations, making internal transfers much more efficient than any long-range shipping, building more momentum to return production to local sources. Renewable energy sources are rarely exportable, and less concentrated in a few states than today's hydrocarbon fuel sources. Replacing energy production and consumption within jurisdictions furthers the tendency to collocate productive capacities near these sources, creating a more balanced economic ecosystem within a state over the long run, and one less vulnerable to cybered coercion campaigns manipulating underlying economic markets.

These disruptive technologies can be distorted, but overall their tendencies, coevolving with the rise of cyber Westphalian borders, will encourage the stakeholders of states to

build the elements of greater economic autarchy within their cyber jurisdictions. That cyberspace itself now has national sections that must be defended will in any case spur local technological innovations and expenditures. The extent that these innovations can be adapted on smaller scales to protect new productive capacity is a collateral benefit likely to enhance technological autarchy as well. That is not to say that like-minded states will not share these technologies and designs, thus furthering the likely compatibility of these rising virtual borders. On the contrary, it is likely they will do so among allies, if only for efficiency reasons. However, for the nearer future, tendencies to be more autarchic in the economic and technological arenas most under attack today and most vulnerable to coercion are likely to prevail.

The harder it is to easily acquire goods or leverage using cyberspace, the more the unpaid or less skilled actors will drop out of cybered operations other than those they need themselves for survival. The transition from the frontier period to the structured cyber Westphalia, however technologically implemented, could also conceivably induce a return to roughly pre-cybered forms of explicit coercion by states with recognised cyber power. These states may or may not be the top two or three economic powerhouses, but they will not be the poorest either. They will have developed the necessary internal systemic resilience to defeat punitive or hostile counter-resilience campaigns and also the forward disruptive capabilities to either punish other coercers or engage in coercion behaviours under their initiative. The costs and difficulty of a deceptive and opaque cybered coercion campaign indirectly shaping systems and inducing behaviours may, for those states, not be worth the effort. If they are relatively secure in themselves, they may return to the pre-cyber and pre-Cold War days of simply making demands for changes in behaviour.

For most states, however, this fortuitous combination of being resilient and able to disrupt as desired may not be achievable or, at least, may not be easily or completely achievable. Their capacities as cyber powers will be heavily determined by how their own versions of a border defending their national jurisdiction are designed, implemented, maintained, adapted, and resourced. For them, in a very real high politics sense, stateness will be measured largely by their systemic national cyber resilience. In any case, for the next ten to fifteen years of transition, all states will need to develop resilience and disruption capacities in balance so that, as the borders rise, they are among the robust cyber powers whose economic stateness enables resistance. There are, so far, no guarantees.

References

Allen, Peter D., and Chris Demchak. 2003. The Palestinian-Israeli Cyberwar. *MILITARY REVIEW* 83 (2): 52-59.

Appelbaum, Richard P., and William I. Robinson. 2005. *Critical Globalization Studies*. London: Routledge.

Baldwin, David Allen. 1985. *Economic statecraft*. Princeton University Press.

Bambauer, Derek E. 2009. Cybersieves. *Duke Law Journal* 59 (3): 377-595.

Benkler, Yochai. 2006. *The wealth of networks: How social production transforms markets and freedom*. Yale University Press.

Blanchard, Jean-Marc F., and Norrin M. Ripsman. 2008. A political theory of economic statecraft. *Foreign Policy Analysis* 4 (4): 371-398.

Blanchard, Jean-Marc F., Edward D. Mansfield, and Norrin M. Ripsman. 1999. The political economy of national security: Economic statecraft, interdependence, and international conflict. *Security Studies* 9 (1-2): 1-14.

Brenner, Joel. 2011. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. Penguin. com.

Buxbaum, Peter A., 2010. 'Battling Botnets.' In *Military Information Technology*. online, 12 (May 13).

Clarke, Richard A., and Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco Books.

Comfort, Louise, Arjen Boin, and Chris Demchak, eds. 2010. *Designing Resilience: Preparing for Extreme Events*. Pittsburgh: University of Pittsburgh Press.

De Janvry, Alain. 1981. *The agrarian question and reformism in Latin America*. Johns Hopkins University Press Baltimore.

Deibert, Ronald. 2012. The Growing Dark Side of Cyberspace (... and What To Do About It). *Penn. St. JL & Int'l Aff.* 1: 260-390.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace*. McClelland & Stewart.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2012. *Access contested: security, identity, and resistance in Asian cyberspace*. The MIT Press.

Demchak, Chris C. 2011. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, Georgia, USA: University of Georgia Press.

———. 2012. 'Resilience, Disruption, and a "Cyber Westphalia": Options for National Security in a Cybered Conflict World.' In *Securing Cyberspace: A New Domain for National Security*, ed. Nicholas Burns and Jonathon Price. Washington, DC: The Aspen Institute.

Demchak, Chris C., and Peter J. Dombrowski. 2011. Rise of a Cybered Westphalian Age *Strategic Studies Quarterly* 5 (1): 31-62.

Denning, Dorothy E. 2010. Cyber Conflict as an Emergent Social Phenomenon. *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. IGI Global*: 170-186.

Dobbin, Frank, Beth Simmons, and Geoffrey Garrett. 2007. The global diffusion of public policies: Social construction, coercion, competition, or learning? *Annual Review of Sociology* 33: 449-472.

Dombrowski, Peter J., and Chris C. Demchak. 2014. Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs, special issue on cyber.*

Drezner, Daniel W. 2003. The hidden hand of economic coercion. *International Organization*: 643-659.

Eaton, Jonathan, and Maxim Peter Engers. 1999. Sanctions: some simple analytics. *American Economic Review* 89 (2): 409-414.

ENISA. 2013. *National Cyber Security Strategies*. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world: European Network and Information Security Agency, European Union.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. 2010. *W32.Stuxnet Dossier: version 1.3*. online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf: Symantex Inc.

Farer, Tom J. 1985. Political and Economic Coercion in Contemporary International Law. *The American Journal of International Law* 79 (2): 405-413.

Farwell, James P., and Rafal Rohozinski. 2011. Stuxnet and the future of cyber war. *Survival* 53 (1): 23-40.

Finkle, Jim. 2010. 'Inside a global cybercrime ring.' In: Reuters.

Gartzke, Erik, and Quan Li. 2003. War, peace, and the invisible hand: Positive political externalities of economic globalization. *International Studies Quarterly* 47 (4): 561-586.

Gellner, Ernest. 1992. *Postmodernism, reason and religion*. Psychology Press.

Gilman, Nils, Jesse Goldhammer, and Steven Weber. 2011. *Deviant globalization: Black market economy in the 21st century*. New York: Continuum.

Glenny, Misha. 2011. *Dark Market*. New York: Random House.

Goldman, Emily. 2010. *Power in Uncertain Times: Strategy in the Fog of Peace*. Stanford University Press.

Goodin, Dan. 2010a. 'Almost 2,500 firms breached in ongoing hack attack: Zeus and Waledac unite in global botnet.' In *El Register*. online.

———. 2010b. 'Upstart crimeware wages turf war on mighty Zeus bot: All your bots belong to us.' In *El Register*. online.

Gross, Michael J. 2011. 'Stuxnet Worm: A Declaration of Cyber-War.' *Vanity Fair*, April, online.

Hamill, Jasper. 2013. 'Chancellor snubs infosec snubs, opens Blighty's kimono.' In *The Register* online www.theregister.co.uk/2013/10/14.

Hanson, Victor D. 2001. *Carnage and culture*. New York: Doubleday.

Hanzhang, Tao. 2007. *Sun Tzu's art of war: the modern Chinese interpretation*. Sterling Publishing Company.

Inkster, Nigel. 2010. China - Threat or Target. *Montrose Journal* 10 (Christmas).

Jentleson, Bruce. 2006. Coercive Diplomacy: Scope and Limits in the Contemporary World. *The Stanley Foundation*.

Keegan, John 2004. *Intelligence in war: knowledge of the enemy from Napoleon to al-Qaeda*. London: Hutchinson

Keohane, Robert Owen, and Joseph S. Nye. 1977. *Power and interdependence: World politics in transition*. Little, Brown Boston.

Lawton, George. 2009. On the trail of the conficker worm. *Computer* 42 (6): 19-22.

Lenway, Stefanie Ann. 1988. Between war and commerce: economic sanctions as a tool of statecraft. *International Organization* 42 (2): 397-426.

Mallery, John C. 2011 (2009). 'A Strategy for Cyber Defense (earlier title: Multi-spectrum Evaluation Frameworks and Metrics for Cyber Security and Information Assurance).' Presented at the MIT/Harvard Cyber Policy Seminar, Cambridge, MA.

Mandiant, APT. 2013. *APT1 Report: Exposing One of China's Cyber Espionage Units (Feb. 2013)*. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Mansfield-Devine, Steve. 2012. Estonia: what doesn't kill you makes you stronger. *Network Security* 2012 (7): 12-20.

Manyika, James, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. 2013. *McKinsey Global Institute Report: Disruptive technologies: Advances that will transform life, business, and the global economy*. http://www.mckinsey.com/insights/business_technology/disruptive_technologies: McKinsey Global Institute.

McGregor, James. 2012. *No Ancient Wisdom, No Followers: The Challenges of Chinese Authoritarian Capitalism*. Prospecta Press.

Miller, John H., and Scott E. Page. 2007. *Complex adaptive systems*. Princeton Univ. Press.

MIT_Physics. 2013. Blog: Security Flaw Shows Tor Anonymity Network Dominated by Botnet Command and Control Traffic. *MIT Technology Review* http://m.technologyreview.com/view/519186/security-flaw-shows-tor-anonymity-network-dominated-by-botnet-command-and-control/.

Morgan, T. Clifton, and Valerie L. Schwebach. 1997. Fools suffer gladly: the use of economic sanctions in international crises. *International Studies Quarterly* 41 (1): 27-50.

Mumford, Enid. 2000. A socio-technical approach to systems design. *Requirements Engineering* 5 (2): 125-133.

Nye Jr, Joseph S. 2011. *The Future of Power in the 21st Century*. Cambridge, MA: Public Affairs.

O'Connell, Robert L. 1989. *Of Arms and Men: A History of War, Weapons, and Aggression*. London: Oxford University Press.

Olson, Parmy. 2012. *We are anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*. Hachette Digital, Inc.

Paganini, Pierluigi. 2013. 'Cyber-espionage: The greatest transfer of wealth in history.' *H+ Magazine online*, March 01.

Palmer, Glenn, and T Clifton Morgan. 2011. *A theory of foreign policy*. Princeton University Press.

Ponemon_Institute. 2012. *Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles*. http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html Hewlett Packard Research.

Rheingold, Harold 1993. *Virtual Communities: Homesteading on the Electronic Frontier*. Reading, UK: Addison Wesley.

Russell, Frank S. 1999. *Information Gathering in Classical Greece*. Ann Arbor: University of Michigan Press.

Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*: Cambridge University Press.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. 2013. 'The Dragon and the Computer: Why Intellectual Property Theft is Compatible with Chinese Cyber-Warfare Doctrine.' In *Introduction to Cyber-Warfare: A Multidisciplinary Approach* eds. Paulo Shakarian, Jana Shakarian and Andrew Ruef. New York: Syngres.

Summerton, Jane. 1994. *Changing Large Technical Systems*. Boulder, Colorado: Westview Press.

Tainter, Joseph. A. 2006. Social complexity and sustainability. *Ecological Complexity* 3 (2): 91-103.

Tilly, Charles. 1992. *Coercion, Capital, and European States, Ad 990-1992*. Cambridge, MA: Blackwell Pub.

USCC. 2012. *US Chamber of Commerce Annual Report to Congress (includes discussion of Chinese hacking)*. http://www.uscc.gov/annual_report/2012/2012-Report-to-Congress.pdf: US Chamber of Commerce.

Walker, Brian, and David Salt. 2006. *Resilience Thinking: Sustaining Ecosystems And People in a Changing World*. Island Press.

Waltz, Kenneth N. 1979. *Theory of international politics*. McGraw-Hill.

Zittrain, Jonathan L. 2006. The generative internet. *Harvard Law Review*: 1974-2040.

Robin Geiß & Henning Lahmann

Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention

1. Introduction

In recent years, international cyber security has become one of the most hotly discussed topics of international law, not only because inter-State cyber security incidents have grown in number and severity, but also because of the realisation that the technical peculiarities of cyberspace pose new and unique legal problems that previously have not been encountered. Thus far, however, inter-State cyber security has unfortunately been treated predominantly as a military issue and as a consequence debate has, by and large, revolved around the question of whether, and under which conditions, measures of self-defence pursuant to Article 51 of the *Charter of the United Nations* (UN Charter) are feasible and permitted in response to a cyber attack. This chapter argues that, while self-defence certainly cannot be ruled out, the problem of attribution will preclude its proper application in many, if not most, instances. Therefore, two other remedies will be analysed that might present an alternative to the prevalent military paradigm of international cyber security: countermeasures and the state of necessity. The chapter provides an outlook on the possibilities of a more comprehensive approach to contemporary security issues that focuses on prevention rather than repression, drawing on States' international due diligence obligations not to harm others.

2. Cyber Security and the Military Paradigm: Self-Defence

2.1 Cyber Attacks as Armed Attacks

So far, both academic and political discussion concerning inter-State cyber threats has focused on whether a State which is the victim of a cyber attack (in the meaning of malicious cyber activities) may respond with force by invoking its inherent right to act in self-defence against the attacker State, or other attacking entity.[1] For such

[1] Antolin-Jenkins, 2005, Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?, 51 *Naval Law Review* 132; Barkham, 2001, Information Warfare and International Law on the Use of Force, 34 *New York University Journal of International Law & Politics* 57; Hoisington, 2009, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, 32 *Boston College International & Comparative Law Review* 439; Jensen, 2002, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 *Stanford Journal of International Law* 207; Kesan/Hayes, 2012, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 *Harvard Journal of Law & Technology* 429; Li, 2013, When Does Internet Denial Trigger the Right of Armed Self-Defense?, 38 *The Yale Journal of International Law* 179; Lin, 2010, Offensive Cyber Operations and the Use of Force, 4 *Journal of National*

acts to be lawful under Article 51 of the UN Charter, the cyber attack would not only have to be considered a use of force within the meaning of Article 2(4) of the UN Charter, but moreover amount to an armed attack. While traditionally the definition of the term 'armed attack' as laid down in Article 51 would have involved a notion of kinetic force,[2] hence following an instrumental approach that primarily centred upon the means of conduct, such an approach has been almost unanimously rejected in the academic literature dealing with cyber attacks. As this form of conduct, by definition, does not employ kinetic force, limiting 'armed attack' to harm caused by traditional military means would plainly mean that a cyber attack could never be regarded as an armed attack, a conclusion obviously unreasonable considering the potential damage done by cyber attacks. Thus, most commentators today agree that the focus of attention should lie not on the means but on the consequences of an attack, and the common denominator is that of equivalence: a cyber attack amounts to an armed attack within the scope of Article 51 if its effects are equivalent to those caused by a conventional attack employing kinetic force.[3] Thus, whenever the use of cyber means for malicious ends leads to considerable physical damage or even to the injury or death of people, that attack has been 'armed', and as a consequence triggers the right of self-defence of the victim State. This approach is hardly new: absent kinetic force, the use of biological or chemical weapons could never have been considered an armed attack without this particular line of argument.[4]

Apart from this general consensus, a few voices seek to broaden the scope of 'armed attack' to include attacks whose effects are not equivalent to consequences of the employment of kinetic force, but remain purely within the realm of cyberspace. Drawing an analogy with naval blockades, Li, for instance, argues[5] that 'DDoS [Distributed Denial of Service] attacks can be categorised as armed attacks for *jus ad bellum* purposes if their impacts on the victim State are sufficiently severe', even in cases where

Security Law & Policy 63; Roscini, 2010, World Wide Warfare - Jus ad bellum and the Use of Cyber Force, 14 *Max Planck United Nations Yearbook* 85; Schmitt, 1999, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 *Columbia Journal of Transnational Law* 885; Schmitt, 2012, Cyber Operations and the Jus Ad Bellum Revisited, 56 *Villanova Law Review* 569; Sklerov, 2009, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 *Military Law Review* 1; Stein/Marauhn, 2000, Völkerrechtliche Aspekte von Informationsoperationen, 60 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 1; Waxman, 2011, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 *The Yale Journal of International Law* 421.

2 Benatar, 2009, The Use of Cyber Force: Need for Legal Justification? 1 *Goettingen Journal of International Law* 375, 389; Woltag, 2010, Cyber Warfare, in Wolfrum (ed.), *Max Planck Encyclopaedia of Public International Law*, Oxford, at para. 8.

3 Schmitt, *op. cit.*, 1999, 913, Roscini, *op. cit.*, 106; Woltag, *op. cit.*, para. 8; Waxman, *op. cit.*, 431 *et seq.*; Joyner/Lotrionte, 2001, Information Warfare as International Coercion: Elements of a Legal Framework, 12 *European Journal of International Law* 825, 863, Keber/Roguski, 2011, Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis, 49 *Archiv des Völkerrechts* 399, 408 *et seq.*

4 Brownlie, 1963, *International Law and the Use of Force by States*, Oxford, 362.

5 Li, *op cit.*, 215.

no physical harm is done. Still further from the prevalent view, Melnitzky makes a rather far-fetched attempt to include even cyber espionage that involves data theft as an armed attack justifying self-defence measures.[6] However, both arguments overstretch by far the possible reach of the term 'armed attack'. To consider any cyber operation that involves some sort of malicious intent as an armed attack within the meaning of Article 51 of the UN Charter not only blurs the lines between this notion and the equally internationally prohibited intervention into other States' affairs with coercive means, but moreover contains the potential for dangerous and premature escalation of conflicts that could and should be solved peacefully.

2.2 The Problem of Attribution

Apart from the precise definition of 'armed attack' within the cyber context, the greatest challenge for the application of the doctrine of self-defence to the new threats that arrive as a by-product of technological developments is the attribution of 'unlawful conduct'. In 1987, the Iran-United States Claims Tribunal asserted that '[i]n order to attribute an act to the State, it is necessary to identify with reasonable certainty the actors and their association with the State'.[7] The second part of this construction – the association of a natural person with a State – is legally governed by Part One, Chapter II of the International Law Commission (ILC) *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (ILC Articles on State Responsibility), Articles 4 to 11. In principle, no specific issues arise here that would not also be found in situations with no connection to cyberspace. The crucial problem is rather hinted at in the first part of the Tribunal's assertion: the identification of the actor. As the technical peculiarities of cyberspace make it entirely possible to hide one's own identity and to obliterate the traces of one's actions, how can we ever know who carried out an attack? If it cannot be determined which individual has acted, then the provisions on the attribution of such conduct found in the Articles on State Responsibility are not of much use.

The problem of the identification of the actor is of course primarily a question of fact, but there is a legal matter tied to it: the question of the standard of evidence. To what degree does responsibility for a particular cyber attack need to be proven? While the burden of proof might be considered unambiguous – in the words of the ILC, in 'a bilateral dispute over State responsibility, the onus of establishing responsibility lies in principle on the claimant State'[8] – the amount or quality of evidence needed in order

6 Melnitzky, 2012, Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses, 20 *Cardozo Journal of International & Comparative Law* 537, 566.

7 *Yeager v Islamic Republic of Iran*, (1987) U.S.C.T.R 17, 92, 101-2.

8 International Law Commission (ILC) Commentaries, Chapter V, at para. 8; Wolfrum, 2012, International Courts and Tribunals, Evidence, in Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, at para. 70; Green, 2009, Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice, 58 *ICLQ* 163, 166.

to establish a fact as given is less clear.[9] Four formalised standards can nonetheless be identified in international courts' and tribunals' jurisprudence in matters concerning State responsibility, and thus also the question concerning responsibility for an armed attack. Those are: the *prima facie* possibility of an asserted fact being true; a preponderance of evidence; the 'clear and convincing' evidentiary standard; and proof beyond reasonable doubt.[10] While it is arguably preponderance of evidence that is the prevailing standard to be met in international litigation in general,[11] as soon as State responsibility is involved the required threshold appears to be considerably higher, shifting towards 'clear and convincing'.[12] This standard essentially amounts to the duty to 'convince the arbiter in question that it is *substantially* more likely than not that the factual claims that have been made are true.'[13] This general pattern seems to have been adopted by the International Court of Justice (ICJ), which generally follows the principle that the more grave an allegation against a State, the higher the standard of proof needs to be.[14] The assertion that another State has not only violated the prohibition on the use of force but has even carried out an armed attack pursuant to Article 51 of the UN Charter is an allegation of considerable gravity. Accordingly, it may be inferred from the leading ICJ case law on the subject – *Nicaragua, Oil Platforms*, and *Armed Activities* – that the test which the Court implicitly applied, when determining whether a situation justifying self-defence had existed, was the standard of 'clear and convincing' evidence.[15] Aside from the Court's jurisprudence, other tribunals' decisions as well as more general State practice confirm this standard as prevalent concerning evidentiary requirements when asserting another State's responsibility or more specifically when claiming a right to use force in self-defence.[16]

---

9 O'Connell, 2002, Evidence of Terror, 7 *Journal of Conflict and Security Law* 19, 21.

10 Green, 2009, *op cit.*, 166 *et seq.*; O'Connell, 2002, *op cit.*, 22; O'Connell, 2006, Rules of Evidence for the Use of Force in International Law's New Era, 100 *Proceedings of the American Society of International Law* 44, 45; Wolfrum, 2012, *op cit.*, at para. 75, however only identifies 'proof beyond reasonable doubt' and 'preponderance of evidence' as frequently used; Kolb, 2006, General Principles of Procedural Law, in Zimmermann (ed.), *The Statute of the International Court of Justic*, at para. 62, lists three while omitting the 'clear and convincing' evidentiary standard.

11 Wolfrum, *op cit.*, , at para. 77.

12 *The Trail Smelter Arbitration Case* (United States of America v. Canada) (1941), 3 RIAA 1905, 1963-65; *Velásquez Rodríguez Case*, Inter-American Court of Human Rights, Judgment of 29 July 1988, at para. 129.

13 Green, 2009, *op cit.*, 167 (emphasis in the original).

14 Benzing, 2010, *Das Beweisrecht vor internationalen Gerichten und Schiedsgerichten in zwischenstaatlichen Streitigkeiten*, Berlin, 516.

15 ICJ, *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA) (Merits)*, Judgment of 27 June 1986, at para. 29; ICJ, *Case Concerning Oil Platforms (Iran v. USA)*, Judgment of 6 November 2003, at paras. 61, 64, 71, 76; ICJ, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, Judgment of 19 December 2005, at para. 136; Green, *Fluctuating Standards*, 172; O'Connell, *Evidence of Terror*, 23.

16 O'Connell, 2006, *op cit.*, 45; see e.g. Eritrea Ethiopia Claims Commission, Partial Award: Jus Ad Bellum (Ethiopia's Claims 1-8), 19 December 2005, at para. 12; for relevant State practice see e.g. Ruys, 2005, *op cit.*, 424 *et seq.*; Green, 2009, *op cit.*, 173 *et seq.*; O'Connell, 2002, *op cit.*, 20, 25-28; Franck, 2006, Reflections on Force and Evidence, 100 *Proceedings of the American Society of International Law* 51, 54; Lobel, 1999, The

The ensuing question must thus be what the requirement to produce 'clear and convincing' evidence means in the cyber context. In view of the technical peculiarities of cyberspace, how likely is it to assume that it will be possible for a State that has become the victim of a cyber attack to sufficiently prove authorship? In recent years, several studies have eroded the hitherto prevalent assumption that the issue of identification in cyberspace is one that will eventually simply be solved by new technical developments.[17] Even almost fifteen years after the first ground-breaking legal study on the topic,[18] 'the determination of the identity or location of an attacker or an attacker's intermediary'[19] remains the most critical and to date unresolved obstacle to the application of the traditional regime of self-defence in the context of cyberspace. The reason for this has not changed: cyber infrastructure was never designed for tracking and tracing user behaviour.[20] Furthermore, software, either 'benign' or 'malicious', consists of nothing but code which, as a representation of data, is entirely capable of being manipulated in just about any measure.[21] The current architecture of the internet and connected networks provides countless loopholes and methods to mask a user's identity or location; online identities and servers can be hidden, data packet flows and connections can be masked and redirected through multiple servers, and an attacker can hijack a machine belonging to an unaware, innocent individual or organisation in order to use it as a basis for launching cyber attacks.[22] Because of those characteristics, reasonably sophisticated attackers will most often be able to effectively hide their traces. Even if an attacking computer can be located with sufficient certainty, what remains is the factor which commentators have called the 'human machine gap'[23] or 'entry-point anonymity':[24] the location of a computer rarely allows for definite conclusions regarding the identity of the individual operating the machine, and it is the latter's status that ultimately determines attribution pursuant to Articles 4 to 11 of the ILC Articles on State Responsibility.

At the same time one cannot *prima facie* rule out the possibility that, at least sometimes, a factual claim concerning authorship of a malicious network operation can be legally

Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan, 24 *Yale Journal of International Law* 537.

17 Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, 1 Sep 2009, available at: http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/.

18 Schmitt, 1999, *op cit*., 885.

19 Hunker, Hutchinson, Margulies, 2008, Attribution of Cyber Attacks on Process Control Systems, in Papa/Shenoi (eds.), *Critical Infrastructure Protection II*, New York/Heidelberg, 87, 88.

20 Lipson, 2002, *Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues*, Carnegie Mellon Software Engineering Institute, available at: http://www.sei.cmu.edu/library/abstracts/reports/02sr009.cfm, 13-15.

21 Gaycken, Krieg der Rechner, *Internationale Politik*, März/April 2011, 88, 92.

22 Information Warfare Monitor, *op. cit.,* 12.

23 Gaycken, *op. cit.*, 94; *Schneier, Anonymity and the Internet*, Schneier on Security, 3 February 2010, available at: http://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html.

24 Lipson, *op. cit.,* 56.

established. In those cases, the 'traditional' rules governing the use of force would apply. However, so far even the most publicly endorsed instances of 'smoking gun' evidence regarding malicious cyber conduct have been met with reservations and objections by high-profile cyber security analysts. This includes the widely reported 'undeniable' proof of China's direct involvement in malicious cyber activity against the United States (US).[25] Even if research such as that undertaken for the Mandiant study does eventually sufficiently prove authorship, it cannot be overlooked that it took their analysts several years to come up with conclusions that they themselves considered sufficiently convincing to be published.[26] Had the allegedly Chinese activity actually been a cyber attack, reaching the threshold of an armed attack within the scope of Article 51 of the UN Charter only several years after the event, could the victim have responded with force invoking self-defence after such a period of time? The recently completed *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn Manual),[27] points to the requirement of immediacy for self-defence to be permitted, meaning the period of time 'following the execution of an armed attack within which the victim State may reasonably respond in self-defence',[28] with one relevant factor *inter alia* being 'the period necessary to identify the attacker'.[29] In cases where 'the initiator of the attack is not identified until well after the attack' the criterion of immediacy will usually not be met.[30] However, the Tallinn Manual suggests that this conclusion may change if there is reason for the victim State to believe that 'further cyber operations are likely to follow' – in that case, the State 'may treat those operations as a "cyber campaign" and continue to act in self-defence'.[31] According to this reasoning, the time span necessary to identify the attacker becomes less significant for the immediacy criterion even if it takes years to gather conclusive evidence, because '[i]f attacks can be accumulated, then a response will satisfy the immediacy requirement even if it comes too early or too late to repel the

25 Mandiant, *APT1 – Exposing One of China's Cyber Espionage Units*, Mandiant, 2013, available at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; Minnick, *China Cyberwarfare Evidence Now Undeniable – Mandiant, Intercepts*, The Official Blog of Defense News International, 19 February 2013, available at: http://blogs.defensenews.com/intercepts/2013/02/china-cyberwarfare-evidence-now-undeniable-mandiant/; Sanger, Barboza, Perlroth, 2003, Chinese Army Unit Is Seen as Tied to Hacking Against U.S., *New York Times*, 19 Feb, p. A1; for criticism see Carr, 2013, *Mandiant APT1 Report Has Critical Analytic Flaws*, 19 Feb, available at: http://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html; Taylor, 2013, Sorry, But That 'Chinese' Hacking Report Proves Nothing, *Business Insider* [online], 19 Feb, available at: http://www.businessinsider.com/mandiant-china-report-questioned-2013-2.

26 See Mandiant Report, Executive Summary, at 2: the firm's investigations had started in 2004; in 2010, a first report was issued, stating that 'The Chinese government may authorise this activity, but there's no way to determine the extent of its involvement.' It took another three years for the analysts to, on their own account, gather 'the evidence required to change our assessment'.

27 International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, ed. by Michael N. Schmitt, Cambridge 2013.

28 Tallinn Manual, at 66.

29 *Ibid*.

30 *Ibid*.

31 *Ibid*.

single incident which prompted it.'[32] While being a reasonable assertion on the face of it, this statement points to a dangerous development. With regard to the US and its allies' 'war on terrorism' after 11 September 2001, which is essentially based on the same legal argument,[33] it has been observed that such a reading of the immediacy criterion 'undermines the temporal dimension of self-defence and risks turning a temporal right into an open-ended licence to use force'.[34] In particular within the cyber context, the issue of uncertain attribution together with a softening of the immediacy requirement could critically raise the danger of escalation of inter-State conflict. Hence, the community of States should continue to demand a more stringent temporal proximity between an armed attack and its response invoking self-defence.

2.3 Suggestions to Alter the Legal Standards Regarding Evidence and Attribution Should Be Discarded

The looming attribution dilemma that might result in the inapplicability of the doctrine of self-defence in many scenarios has led to various scholarly attempts to find legally valid alternatives. So far, most of those arguments have directly tackled the rules of attribution or evidence. However, they either do not manage to solve the problem, or they find no basis in current international law. The suggestion[35] that the standards of attribution should shift from 'effective control'[36] to 'overall control'[37] does not touch upon the issue of identification.[38] Deliberations that aim to lower the evidentiary standard regarding cyberspace issues, emphasising the *ex-ante* perspective of decision-makers in emergency situations,[39] or even bluntly asserting that the requirement of adequate attribution of an attack before resorting to self-defence measures is 'a luxury unavailable in the cyber attack era',[40] can hardly be considered legally tenable. There is widespread agreement that international law as it currently stands applies in cyberspace,[41] and it is

32 Tams, 2009, The Use of Force Against Terrorists, 20 *European Journal of International Law* 359, 390.

33 See e.g. Schmitt, 2003, Preemptive Strategies in International Law, 24 *Michigan Journal of International Law* 513, 535 *et seq*; Sklerov, 2009, *op cit.*, 36.

34 Tams, 2009, *op. cit.*, 389.

35 Shackelford, 2009, From Nuclear War to Net War: Analogising Cyber Attacks in International Law, 27 *Berkeley Journal of International Law* 191, 235.

36 ICJ, *Nicaragua*, at paras. 105-115.

37 ICTY, Appeals Chamber, Tadić, 15 July 1999 (Case no. IT-94-1-A), at para. 120.

38 On the so-called 'unwilling or unable' doctrine in relation to self-defence, see below.

39 Tallinn Manual, *op cit.*, at 60.

40 Jensen, 2002, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 *Stanford Journal of International Law* 207, 232; Condron, 2007, Getting It Right: Protecting American Critical Infrastructure in Cyberspace, 20 *Harvard Journal of Law & Technology* 403, 415; Hoisington, 2009, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, *32 Boston College International and Comparative Law Review* 439, 452 *et seq*.

41 See speech delivered by Harold Hongju Koh, International Law in Cyberspace, 18 September 2012, available at: http://www.State.gov/s/l/releases/remarks/197924.htm.

beyond any doubt that international law requires attribution.[42] Regarding the *ex-ante* perspective as critical might considerably undermine the *jus contra bellum*, as past cases have shown that this angle is structurally insufficient when it comes to the identification of cyber attacks. Finally, suggesting a reversal of the burden of proof could easily lead to wrong and even absurd results given the possibility of routing cyber operations through numerous countries, and to the denouncing of wholly uninvolved and innocent States.[43]

2.4 Interim Conclusion

It is now generally accepted that cyber attacks can reach the armed attack threshold stipulated in Article 51 of the UN Charter, thus triggering the right of self-defence which justifies an armed response, be it in return via cyberspace or carried out with more traditional means. However, while this finding holds true in principle, the standard of proof required by international law when making claims that involve another State's responsibility (especially for an armed attack) in combination with the technical peculiarities of cyberspace will, in at least the majority of cases, effectively prevent the legal possibility of reaction with military means. All the arguments so far suggested which attempt to 'circumvent' the problem are unconvincing. Still, it cannot be denied that inter-State cyber attacks already occur, and will most likely increase in number in the future. Therefore, it cannot be enough simply to point to the near inapplicability of the self-defence doctrine: to meet States' legitimate security interests, it is necessary to seek alternatives. Feasible solutions to the problem will not be found within the self-defence regime, but beyond the military paradigm that underpins the focus on self-defence. Hence, in the following section, two other legal concepts are analysed which, alongside self-defence, are listed as circumstances precluding wrongfulness in the ILC Articles on State Responsibility: countermeasures and necessity.

3. Beyond the Military Paradigm: Countermeasures and Necessity

3.1 Countermeasures

3.1.1 Function and Preconditions of Countermeasures

The first remedy apart from self-defence for a State which finds itself under attack through cyberspace is to resort to a countermeasure. According to Article 22 of the ILC Articles on State Responsibility, '[t]he wrongfulness of an act of a State not in

42 Green, 2009, *op cit.*, 169 *et seq.*

43 Conference proposal, cited by Ziolkowski, 2012, *Ius ad bellum* in Cyberspace - Some Thoughts on the 'Schmitt-Criteria' for Use of Force, in Ziolkowski *et al.* (ed.), 2012 4th *International Conference on Cyber Conflict – Proceedings*, Tallinn, 295, 307; Ziolkowski mentions the Stuxnet attack, which involved command and control servers located in countries such as Denmark and Malaysia, States that were clearly wholly unaware of the operation.

conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State'. Countermeasures may be defined as 'pacific unilateral reactions which are intrinsically unlawful, which are adopted by one or more States against another State, when the former considers that the latter has committed an internationally wrongful act which could justify such a reaction'.[44] The function of such measures under the current state of international law is twofold. Firstly, as described by Article 22, they act as a circumstance precluding the wrongfulness of the deliberately chosen conduct of a State that would otherwise be contrary to its international obligations and hence trigger its responsibility. At the same time countermeasures are a means of triggering the responsibility of the adversary State.[45] As such, they are appropriately described as 'law enforcement measures which consist of a temporary dispensation from complying with the law'.[46] International practice confirms the existence of countermeasures as circumstances precluding the wrongfulness of otherwise unlawful conduct,[47] and in its *Gabčíkovo-Nagymaros Project* case, the ICJ formulated certain preconditions found in customary law[48] that are echoed in the ILC Articles on State Responsibility in Chapter II of Part Three.

For countermeasures to be considered lawful, Article 49(1) of the ILC Articles stipulates that the 'injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations'. This phrasing principally implies two restrictions. First, countermeasures must be aimed at a State that has committed an act that is unlawful under international law. In this sense, countermeasures are akin to self-defence: the determination of a legally responsible actor is a necessary condition of any countermeasure. The main difference is that, unlike self-defence where the other State's unlawful act is predetermined as an 'armed attack', the instrument of countermeasures is valid in response to any wrongful conduct in relation to which it only permits non-forcible responses. It also follows that the countermeasures 'must be directed against that State'.[49] Furthermore, the provision implies the permitted goal of resorting to countermeasures: the conduct must attempt to achieve the responsible State's compliance with the respective obligations and be strictly necessary to that end, that is, the cessation of unlawful conduct.

44 Alland, 2010, The Definition of Countermeasures, in Crawford *et al.* (ed.), *The Law of International Responsibility*, Oxford, 1135.

45 Lesaffre, 2010, Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Countermeasures, in Crawford *et al.* (ed.), *The Law of International Responsibility*, Oxford, at 439 *et seq.*

46 Zoller, 1984, *Peacetime Unilateral Remedies. An Analysis of Countermeasures*, New York, 137.

47 See ILC Commentaries, Article 22, at para. para. 2; Lesaffre, *op cit.*, 470.

48 ICJ, *Gabčíkovo-Nagymaros Project* (*Hungary v. Slovakia*), at paras. 83 *et seq.*

49 *Ibid.*, para. 83.

Countermeasures may not, therefore, be employed in order to punish the adversary.[50] However, the commentary to Rule 9 of the Tallinn Manual notes that State practice is ambiguous in this regard, as States 'sometimes appear to be motivated by punitive considerations when resorting to countermeasures'.[51] In any case, to achieve the goal of restoration of compliance, the injured State is under no obligation to resort to means that 'mirror the underlying wrongful act against which they are directed'.[52] There might be good arguments in favour of a concept of reciprocity with regard to the necessity and proportionality requirements,[53] but the ILC rightly observes that 'a limitation to reciprocal countermeasures assumes that the injured State will be in a position to impose the same or related measures as the responsible State, which may not be so'.[54] As explained below, this assessment is particularly relevant in the cyber context.

Article 50 enumerates certain definite restrictions on countermeasures: they 'shall not affect the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations; obligations for the protection of fundamental human rights; obligations of a humanitarian character prohibiting reprisals; other obligations under peremptory norms of general international law'. So whatever the circumstances of a single case, some superior values of the international legal system may not be impaired by the State that resorts to the instrument.[55] This unambiguous wording notwithstanding, there is a persistent debate surrounding the question of the use of force in legal doctrine and international jurisprudence. In his separate opinion to the ICJ's *Oil Platforms* decision, Judge Simma famously held that 'the permissibility of strictly defensive military action taken against attacks [that remain below the threshold of Article 51 of the UN Charter] cannot be denied'.[56] He considered such actions 'proportionate counter-measures' in reference to a part of the Court's judgments on the merits of the *Nicaragua* case, where the ICJ had held that '[w]hile an armed attack would give rise to an entitlement to collective self-defence, a use of force of a lesser degree of gravity cannot [...] produce any entitlement to take collective countermeasures involving the use of force. The acts of which Nicaragua is accused [...] could only have justified proportionate countermeasures on the part of the State which had been the victim of

50 ILC Commentaries, Article 49, at para. 1; traditionally, reprisals comprised 'a perceived moral right to punish the responsible State's delict', Calamita, 2009, Sanctions, Countermeasures, and the Iranian Nuclear Issue, 42 *Vanderbilt Journal of Transnational Law* 1393, 1420; see on this point critically Bederman, 2002, Counterintuiting Countermeasures, 96 *American Journal of International Law* 817, 822: 'This change in emphasis on the nature and purpose of countermeasures likewise places in some doubt the Commission's use of earlier international law sources.'

51 Tallinn Manual, *op cit.*, at 37.

52 Calamita, 2011, Countermeasures and Jurisdiction: Between Effectiveness and Fragmentation, 42 *Georgetown Journal of International Law* 233, 243.

53 ILC Articles, Commentaries, Part Three Chapter II, at para. 5.

54 *Ibid.*

55 See in general Leben, *op cit.*, 1197 *et seq.*

56 ICJ, *Oil Platforms*, Separate Opinion of Judge Simma, at para. 12.

these acts [...]'.[57] Beyond such 'strictly defensive military action' as advanced by Simma, the possibility of lawful countermeasures employing the use of force cannot be found in State practice in the Charter era since 1945,[58] though as late as 2002, the matter was regarded as 'controversial'.[59] Irrespective of whether or not Simma's argument is in itself a defensible interpretation of the *Nicaragua* judgment and of State practice,[60] this issue might in any case gain new relevance within the cyber context.

According to Article 51 of the ILC Articles on State Responsibility, which is considered to reflect customary international law,[61] countermeasures must also be in line with the principle of proportionality or, in the provision's wording, 'commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question'. Just as in other contexts, the proportionality principle 'is intended to act as a brake on escalating cycles of transactional violence'.[62] The judgment on the question of proportionality is, of course, not static but flexible; one that 'can at best be accomplished by approximation',[63] incorporating considerations of principle as well as material factors.[64] Hence, not only 'quantitative' elements determine proportionality, but also 'qualitative' considerations,[65] including 'the importance of the interest protected by the rule infringed and the seriousness of the breach'.[66]

Procedural questions conditioning the execution of countermeasures are dealt with in Article 52. Before starting to take countermeasures an injured State must, according to the first paragraph, 'call upon the responsible State [...] to fulfil its obligations under Part Two'. Apart from that, the injured State must also 'notify the responsible State of any decision to take countermeasures and offer to negotiate with that State', Article 52(1)(b).

57 ICJ, Nicaragua, at para. 249.

58 Gazzini, 2005, The Changing Rules on the Use of Force in International Law, Manchester, 169; Barsotti, 1986, Armed Reprisals, in Cassese (ed.), *The Current Legal Regulation of the Use of Force*, Dordrecht, 81, 90 *et seq.*; Zimmermann, 2007, The Second Lebanon War: Jus ad Bellum, Jus in Bello and the Issue of Proportionality, 11 *Max Planck Yearbook of United Nations Law* 99, 104 *et seq.*

59 Franck, 2002, *Recourse to Force. State Action Against Threats and Armed Attacks*, Cambridge, 54; the author however observes that despite resembling countermeasures, uses of force by States were mostly labelled as self-defence, 67; see also his analysis of State practice, 109-134.

60 See on this in particular Corten, 2011, Judge Simma's Separate Opinion in the Oil Platforms Case: To What Extent Are Armed 'Proportionate Defensive Measures' Admissible in Contemporary International Law? in Fastenrath *et al.* (ed.), *From Bilateralism to Community Interest. Essays in Honour of Judge Bruno Simma*, Oxford, at 843.

61 O'Keefe, 2010, Proportionality, in Crawford *et al.*, *The Law of International Responsibility, Oxford*, at 1157.

62 Franck, 2008, On Proportionality of Countermeasures in International Law, 102 *AJIL* 715, 715.

63 Case Concerning the Air Services Agreement of 27 March 1946 (United States of America v France), 9 December 1978, 18 RIAA 416, at para. 83.

64 Fisler Damrosch, 1980, Retaliation or Arbitration – or Both? The 1978 United States-France Aviation Dispute, 74 *AJIL* 785, 807.

65 See Klein, 1997, Gegenmaßnahmen, 37 *Berichte der Deutschen Gesellschaft für Völkerrecht* 39, 62.

66 ILC Commentaries, Article 51, at para. 6.

Those are cumulative conditions, the second following the first.[67] In cases of urgency, however, the injured State may take those measures that are 'necessary to preserve its rights', an exception to the abovementioned paragraph 1(b) as stipulated by paragraph 2 of the same Article. Furthermore, according to the third paragraph, countermeasures 'may not be taken, and if already taken must be suspended without undue delay if the internationally wrongful act has ceased, and the dispute is pending before a court or tribunal which has the authority to make decisions binding on the parties'. Finally, due to their purely instrumental character, countermeasures are necessarily time-limited,[68] which *inter alia* entails the duty to terminate the measure 'as soon as the responsible State has complied with its obligations under Part Two in relation to the internationally wrongful act', as prescribed by Article 53 of the ILC Articles on State Responsibility. The inherent limitation in time also entails the 'fundamental condition'[69] to choose such countermeasures that are reversible, as already noted by the ICJ.[70] The ILC qualified the Court's strict wording insofar as it stipulated that countermeasures 'must be as far as possible reversible in their effects',[71] thus reasonably envisaging that complete reversibility will not always be realistic or even possible. More precisely, in the view of the ILC, Article 49(3) merely obliges the injured State to select the measure that is reversible, 'if [it] has the choice between a number of lawful and effective countermeasures'.[72]

3.1.2 Countermeasures in Response to Cyber Attacks

When countermeasures are being considered as unilateral remedies against cyber attacks, different scenarios that each require a different and distinct legal assessment are possible. Hitherto, when commentators took into account countermeasures within cyber attack scenarios, they were mostly motivated by the awareness that not every malicious cyber activity would reach the threshold of an armed attack pursuant to Article 51 of the UN Charter.[73] The same can be said about statements by State representatives.[74] What

67 Kamto, 2010, The Time Factor in the Application of Countermeasures, in Crawford *et al.* (eds.), *The Law of International Responsibility*, Oxford, 1170.

68 *Ibid.*, 1173 *et seq.*

69 *Ibid.*, 1174.

70 ICJ, *Gabčíkovo-Nagymaros Project (Hungary v Slovakia)*, Judgment of 25 September 1997, at para. 87.

71 ILC Commentaries, Part Three, Chapter II, at para. 6.

72 *Ibid.*, Article 49, at para. 9.

73 Stein/Marauhn, *op cit.*, 26; Sklerov, *op cit.*, 36 *et seq.*; Roscini, *op cit.*, 113; Hinkle, 2011, Countermeasures in the Cyber Context: One More Thing to Worry About, 37 *The Yale Journal of International Law* [Online] 11; Hathaway *et al.*, 2012, The Law of Cyber Attack, 100 California Law Review 817, 857 *et seq.*; O'Connell, 2012, *op cit.*, 204; but see Li, 2013, *op cit.*, 211 *et seq.*

74 U.S. Department of Defense, 1999, An Assessment of International Legal Issues in Information Operations, 16 *et seq.*; speech by the Secretary of State of the German Federal Ministry of the Interior, International Co-Operation in Developing Norms of State Behaviour for Cyberspace, Berlin, 13 December 2011, quoted in Krieger, Krieg gegen anonymous. Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar, 50 *Archiv des Völkerrechts* 1, 14 (2012).

is usually envisaged is a function of countermeasures that is akin to self-defence, but reserved for situations where, absent the existence of an armed attack, self-defence is not an option.[75] Hence, protection against an imminent or ongoing cyber attack will be achieved through offensive action – infringing on the rights of another State – justified as a countermeasure in accordance with the provisions as enshrined in the ILC Articles. The frequently mentioned offensive tools in this regard are so-called 'active defences' which, as opposed to 'passive defences' are:

> proactive measure[s] for detecting or obtaining information as to a cyber-intrusion, cyber-attack, or impending cyber operation, or for determining the origin of an operation that involves launching a pre-emptive, preventive, or cyber-counter operation against the source.[76]

In other words, 'active defences' are 'in-kind response[s] [...] against the attacker's system'[77] in order to offensively 'disable the source of an attack'.[78] To their proponents, the advantage of such active defences within the analysed context is that those are logically reciprocal. While reciprocity is not a precondition for the lawfulness of countermeasures, the ILC in reference to the *Air Service Agreement* arbitration[79] nonetheless holds that '[c]ountermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or a closely related obligation'.[80]

The main problem with countermeasures is that, as with self-defence, the remedy is dependent on the attribution of wrongful conduct; the wrongful conduct here not being an armed attack, but rather a cyber attack which violates other international norms such as the prohibition of the use of force pursuant to Article 2(4) of the UN Charter (without reaching the armed attack threshold), or the customary principle of non-intervention. If attribution in order to establish State responsibility of the alleged attacker State is again a precondition, it follows that the same evidentiary standard applies as outlined above.[81] As a consequence, the victim State is confronted with the same legal and factual problems when attempting to establish a legal basis for reacting with active defences.

Contrary to what has been argued by some authors,[82] this conclusion is not altered by the consideration that, in most instances, what the State would actually resort to in

75 But see O'Connell, 2012, *op cit.*, 205, who expressly envisages a different role for countermeasures in the cyber security context.

76 Tallinn Manual, *op cit.*, Glossary of Technical Terms, 257.

77 Sklerov, *op. cit.,* 25.

78 Hathaway, *op. cit.,* 858.

79 Case Concerning the Air Services Agreement of 27 March 1946 (*United States of America v France*), 9 December 1978, 18 RIAA 416.

80 ILC Commentaries, Part Three, Chapter II, at para. 5.

81 See para. 2.2.

82 Hinkle, *op. cit.,* 18 *et seq.*

such an emergency situation are so-called 'urgent countermeasures' as described by Article 52(2) of the ILC Articles on State Responsibility.[83] Indeed, it has been argued that 'international law [...] appears to acknowledge the subjectivity inherent in a State's determination',[84] which in turn means that 'the nature of cyber-force weighs in favour of an injured State resorting rapidly, *and with broad discretion*, to countermeasures'.[85] However, while according to the wording of Article 52, 'the injured State may take such urgent countermeasures as are necessary to preserve its rights', this expressly only exempts it from the obligation detailed in Article 52(1)(b) to '[n]otify the responsible State of any decision to take countermeasures and offer to negotiate with that State'. Thus, what is altered in situations of urgency is only a procedural requirement, not the evidentiary standard required to be able to resort to this remedy in the first place. Therefore, it cannot be concluded that States have a broader discretion when it comes to taking countermeasures in emergency situations triggered by cyber attacks. After all, '[u]rgent countermeasures are nothing but a form of countermeasures in an urgent situation, and their necessity must be shown in a precise manner'.[86] As countermeasures inherently bear the risk of escalating a dispute, when one of the procedural safeguards is abandoned to take urgency into account it becomes even more crucial that the acting State has ascertained the facts that are relied upon as the legal basis for its conduct. It follows that to directly attribute a cyber attack in order to justify active countermeasures is just as difficult as establishing such a link in situations where the initial malicious cyber operation amounted to an armed attack.

Unlike self-defence, responsibility for the attack itself is not the only possible legal link under which countermeasures may be justified. As countermeasures are considered a means of self-help that aim to induce a State responsible for *any* internationally wrongful act to comply with its international obligations according to Article 49(1) of the ILC Articles on State Responsibility, the relevant act (or omission) can also be of a secondary nature. As pointed out by several scholars, countermeasures may thus also be feasible against violations of a legal duty to prevent cyber attacks. The starting point of this conclusion is the consideration that every State has an active duty to prevent cyber attacks against other States that emanate from its own territory.[87] In this context, it should be noted that if a State attempts to justify the employment of active defences as countermeasures as a response to an actual cyber attack, then such a legal constellation

83 Krieger, *op. cit.,* 16.

84 Hinkle, *op. cit.,* 17.

85 *Ibid.*, 18 (emphasis added); see also Elagab, 1988, *The Legality of Non-Forcible Counter-Measures in International Law*, Oxford, 50.

86 Iwasawa & Iwatsuki, 2010, Procedural Conditions, in Crawford *et al.* (eds.), *The Law of International Responsibility, Oxford*, 1149, 1155; likewise Krieger, *op. cit.,* at 16.

87 See e.g. Sklerov, *op. cit.,*70 *et seq.*; Hathaway, *op. cit.,* 879; Roscini, *op. cit.,* 102; Tallinn Manual, *op. cit.,* 26 *et seq.*

as analysed below necessarily creates a situation of non-reciprocity: the internationally wrongful act is not the attack itself but merely the failure to prevent it.

The existence in contemporary international law of a general duty to prevent attacks originating from a State's own territory against the territory and legally protected interests of other States is widely accepted. In its recent *Pulp Mills* decision,[88] the ICJ referred to its earlier case law[89] in order to determine that the principle of prevention is 'a customary rule' that 'has its origins in the due diligence that is required of a State in its territory'.[90] According to the Court, this means that '[a] State is [...] obliged to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State.'[91] While this judgment was concerned with environmental issues – the subject matter going back at least to the *Trail Smelter* arbitration[92] – a duty to prevent harm to other States has been established on a more general scale in international law. In particular, since 1945, the principle has been confirmed by the ICJ in the *Corfu Channel* case, where it was held that every State is under an 'obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[93] The doctrine eventually gained further momentum with the (re-)emergence of non-State violence in the second half of the 20th century, in particular with the rise of transnational terrorism.[94] In 1999 and 2000, the UN Security Council demanded that the Taliban, then Afghanistan's government, abstain from allowing the territory under its control to be used as a basis for terrorist training and planning by *Al Qaeda*,[95] a specific manifestation of the duty to prevent which was reiterated and reinforced after the 11 September 2001 terrorist attacks on the US.[96]

Early on, there were attempts to translate this established principle of a 'duty to prevent' into the cyber realm. In 2000, the UN General Assembly urged States to ensure that 'their laws and practice eliminate safe havens for those who criminally misuse

88 ICJ, *Case Concerning Pulp Mills on the River Uruguay (Argentine v Uruguay*), Judgment of 20 April 2010, at para. 101.

89 Most notably ICJ, *The Corfu Channel Case* (*United Kingdom v Albania*) (Merits), Judgment of 9 April 1949, ICJ Reports 1949, 22; ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, at para. 29.

90 ICJ, *Pulp Mills,* at para. 101.

91 *Ibid.*

92 Trail Smelter case (*United States of America v Canada*), 16 April 1938 and 11 March 1941, 3 RIAA 1905.

93 ICJ, *Corfu Channel*, 22.

94 Heathcote, 2012, State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility, in Heathcote *et al.* (ed.), *The ICJ and the Evolution of International Law. The Enduring Impact of the Corfu Channel Case*, London, 295, 306 *et seq*.

95 UN SC Res. 1267 (15 October 1999); UN SC Res. 1333 (19 December 2000).

96 UN SC Res. 1368 (12 September 2001); UN SC Res. 1373 (28 September 2001); see Barnidge, 2005, States' Due Diligence Obligations with regard to International Non-State Terrorist Organisations Post 11 September 2001: the Heavy Burden that States must bear, 16 *Irish Studies in International Affairs* 103, 110 *et seq*.

information technologies'.[97] The recently completed Tallinn Manual expressly applies the *Corfu Channel* standard to cyber security matters by framing the rule that '[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States'.[98] Still, while there might in fact remain little doubt that such an obligation is to be considered as reflecting the current state of customary international law, the rule's specific content is much less clear. As confirmed by the ICJ in *Pulp Mills*, the 'duty to prevent' finds its roots in, and is more specifically detailed by, a State's due diligence obligations towards other States. Thus, to determine whether a State has violated its duty to prevent a cyber attack against another State, those due diligence obligations must be spelled out. For the time being, it may be sufficient to follow the ICJ's decision in the *Tehran Hostages* case that, at least when a State positively knows of acts on or emanating from its territory that adversely and unlawfully affect the rights and legally protected interests of another State, it is under a specific duty to 'take appropriate steps' in order to prevent harm if it has 'the means at [its] disposal to perform [its] obligations'.[99] That does not necessarily mean that a State has to guarantee that it is able to control every activity within its territory, as was already confirmed by an arbitral tribunal as early as 1925.[100] Instead, such obligations can only be framed as 'best efforts obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur'.[101] In the words of the ICJ, the duty to prevent is an obligation of conduct, not of result.[102] Whatever the exact standard of due diligence is in detail as regards the specific situation at hand, when a State is aware of impending harm and has the means at its disposal to prevent it from occurring and yet remains inactive, it may subsequently be held responsible for its violation of the duty to prevent.

The issue of the exact content of the duty to prevent cyber attacks notwithstanding, the argument under scrutiny is not without further pitfalls. Even if some of the evidentiary issues obstructing the self-defence justification may be avoided when focusing on a State's duty to prevent cyber attacks, the countermeasures approach still faces two considerable, closely interrelated problems that may not be ignored. At first, it follows from the above that a State that is the victim of a cyber attack needs to be able to show two things with clear and convincing evidence: that the attack emanated from the territory

97 UN GA Res. 55/63 (4 December 2000).

98 Tallinn Manual, *op cit.*, 26.

99 ICJ, *Case concerning United States Diplomatic and Consular Staff in Tehran* (*United States of America v. Iran*), Judgment of 24 May 1980, at para. 68.

100 Affaire des biens britanniques au Maroc espagnol (*Espagne v Royaume-Uni*), 1 May 1925, 2 RIAA 615, 640 *et seq.*

101 ILC Commentaries, Article 14, at para. 14.

102 ICJ, *Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina v Serbia and Montenegro*), judgment of 26 February 2007, at para. 430.

of the accused State, and that the State failed in its due diligence obligations under the duty to prevent the attack. Proving the territory of origin might be less problematic than additionally having to establish which individual carried out the attack, but under the conditions of cyberspace this still remains anything but an easy task. Establishing a territorial link to a convincing degree means tracing back the malicious data, and in the words of a technical expert on the issue, 'there is still no "silver bullet" in the hunt for the attackers'.[103] A majority of authors maintains that it is essentially 'impossible to prove' that a State tolerates cyber attacks against other States emanating from its own territory.[104] Even scholars who principally argue in favour of employing active defences acknowledge that the success rate of trace programs is not only imperfect,[105] but is in fact 'inherently limited',[106] so the possibility of incorrect identification of the true source of an attack remains high.

This scholarly assessment is frequently obscured by news reports that suggest otherwise. In May 2013, in a much-noticed annual report to Congress, the US Department of Defense maintained that of the numerous intrusions that had targeted government computers in 2012, 'some [...] appear to be attributable directly to the Chinese government and military'.[107] Besides China, Iran was also openly accused of having conducted or at least tolerated cyber attacks against the US. In the same month, US officials claimed that malicious intrusions into the security control systems of US power companies had been 'unmistakeably' traced back to Iran.[108] While it is virtually impossible to assess the value of the mostly undisclosed evidence linking the attacks to these States, it appears likely that what eventually led to these conclusions was a process not of technical but of 'all-source attribution': a comprehensive approach 'that integrates information from all sources, not just technical sources at the scene of the attack',[109] including intelligence or political sources. For political purposes, this sort

103 Caltagirone, 2005, *Active Response*, University of Idaho, available at: http://www.classstudio.com/scatagi/papers/professional_papers/msthesis/sergioThesis.pdf, 12.

104 See e.g. Gaycken, 2010, The Necessity of (Some) Certainty – A Critical Remark Concerning Matthew Sklerov's Concept of 'Active Defense', 12 *Journal of Military and Strategic Studies* 1; Hollis, 2011, An e-SOS for Cyberspace, 52 *Harvard Journal of International Law* 397-404.

105 Kesan/Hayes, 2012, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 *Harvard Journal of Law & Technology* 482.

106 Wheeler & Larsen, 2003, *Techniques for Cyber Attack Attribution*, Oct 2003, available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859, 51-52.

107 Office of the Secretary of Defense, 2013, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, available at: http://www.defense.gov/pu/2013_china_report_final.pdf, 36.

108 Perlroth/Sanger, New Computer Attacks Traced to Iran, Officials Say, *The New York Times*, [online] 25 May, available at: http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html?_r=o; Gorman/Yadron, 2013, Iran Hacks Energy Firms, U.S. Says, *The Wall Street Journal*,[online] 24 May, available at: http://online.wsj.com/article/SB10001424127887323336104578501601108021968.html.

109 Owens *et al.*, 2009, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, 139.

of attribution may be sufficient,[110] but the same can hardly be said in establishing legal responsibility as long as clear and convincing technical evidence is absent. Ultimately, there remains crucial doubt whether the gathering of such circumstantial evidence can ever lead to truly conclusive results.[111]As regards countermeasures, despite all reports and official statements that imply the contrary, 'definitely attributing' cyber incidents and violations of international law related thereto is still one of the 'greatest strategic challenges regarding cyber threats'.[112]

There may well be cases where identification of territory of origin and thus the establishment of responsibility for a violation of the duty to prevent are in fact possible. However, what again needs to be brought into the equation is the factor of time; this issue is crucial not only as regards self-defence, but also for the employment of countermeasures. According to the prevalent view, the remedy of resorting to countermeasures is strictly instrumental, and not permitted as a means to retaliate. As a consequence, countermeasures are not allowed once the unlawful act has ceased.

A different assessment might be tenable when a State is dealing not with a single attack, but rather with a malicious cyber campaign or a continuous attack rather than a one-off intrusion. In such instances, countermeasures might become useful tools in future cyber security matters. While the violation of the duty to prevent an attack is by itself not an omission extending in time within the meaning of Article 14(3) of the ILC Articles on State Responsibility, the breach of the international obligation may well become continuous when one or more attacks have already occurred, but the territorial State has not implemented any measures to prevent further instances. In accordance with Article 30(a) of the ILC Articles on State Responsibility, an internationally wrongful act is also to be considered 'continuing' for the purpose of these regulations 'where a State has violated an obligation on a series of occasions, implying the possibility of further repetitions'.[113] This connection had already been implied by the ICJ in the *Tehran Hostages* case[114] and also applies to wrongful omissions according to the arbitral tribunal that decided the *Rainbow Warrior* case.[115] Thus, if a series of cyber attacks

110 See Ziolkowski, 2012, *op cit*., 306.

111 See e.g. Markoff *et al*., 2010, In Digital Combat, U.S. Finds No Easy Deterrent, *The New York Times*, [online] 25 Jan, available at: http://www.nytimes.com/2010/01/26/world/26cyber.html, about a cyber attack simulation carried out by the U.S. Department of Defense: 'No one could pinpoint the country from which the attack came.'

112 See the Director of U.S. National Intelligence James R. Clapper, Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, 31 January 2012, available at: http://www.intelligence.senate.gov/120131/clapper.pdf, 8.

113 ILC Articles, Commentaries, Article 30, at para. 3.

114 ICJ, *Tehran Hostages*, *op. cit.,* para. 80.

115 Case Concerning the Difference Between New Zealand and France Concerning the Interpretation or Application of two Agreements, Concluded on 9 July 1986 Between the two States and Which Related to the Problems Arising from the Rainbow Warrior Affair (*New Zealand v. France*), 30 April 1990, 20 RIAA 217, 270, at para. 113.

occurs over a period of time, the chance of being able to obtain sufficient evidence – technical and otherwise – after each instance in order to identify the territory of origin is significantly increased. In such a case, it is not unreasonable to assume that a countermeasure short of the use of force might be launched early enough to meet the requirement of countermeasures to be a strictly instrumental, and not retaliatory tool at the State's disposal. These constrains leave that particular remedy with a considerably limited scope of application.

Proponents of the so-called 'unwilling or unable' doctrine attempt to apply a corresponding rationale to the justification of measures that employ force under self-defence.[116] Although not always made explicit, the doctrine is split into two conceptually different subsets. In the first, either unwillingness or inability lead to the attribution of the armed attack itself, in which case self-defence would be allowed against the territorial State.[117] Here, the argument runs parallel to the one applied to countermeasures above. In the second and seemingly more prevalent view, unwillingness and inability merely lead to the duty of the State to accept and tolerate self-defence measures on its territory conducted directly against the responsible non-State actors.[118] However, this variant struggles to explain the origin of the territorial State's obligation.[119] Disregarding the question of the current status of the doctrine under international law,[120] Tams convincingly argues that the former alternative is the one reflected in contemporary State practice as regards terrorism, as it:

> suggests that a territorial State has to accept anti-terrorist measures of self-defence directed against its territory where it is responsible for complicity in the activities of terrorists based on its territory – either because of its support below the level of direction and control or because it has provided a safe haven for terrorists.[121]

While far from the 'Nicaragua standard' of attribution, this is still a considerably higher threshold than mere 'inability' or 'unwillingness', and thus is more than a violation of a due diligence obligation that might lead to the permissibility of countermeasures short of the use of force. Applying the argument to the cyber security framework, it still seems that to obtain 'clear and convincing' evidence for the identification both of the actor and of State involvement will only rarely be possible, even if it cannot be

116 Deeks, 2012, 'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense, 52 *Virginia Journal of International Law* 483; Schmitt, 2003, Preemptive Strategies in International Law, 24 *Michigan Journal of International Law* 513, 541 *et seq.*; Tallinn Manual, Rule 13, para. 22 *et seq.*

117 Sklerov, *op. cit.,* 13 and 38 *et seq.*

118 In this sense Schmitt, *Preemptive Strategies*, 541 *et seq.*; the Tallinn Manual's position on this matter is ambiguous.

119 For a comparison of both lines of argumentation see Tams, 2009, *op cit.*, 384 *et seq.*

120 See Deeks, *op. cit.,* 546.

121 Tams, 2009, *op. cit.,* 385.

ruled out in principle. This assessment would change if one additionally accepts the closely related 'accumulation of events' doctrine, which asserts that a series of minor incidents taken together might amount to an armed attack.[122] This argument alludes to the continuation of wrongful conduct pursuant to Article 30(a) of the ILC Articles on State Responsibility in connection to countermeasures. However, while this concept is clearly applicable to violations of due diligence obligations, justifying the employment of countermeasures,[123] it would be logically invalid to infer from this that a series of attacks not amounting to an armed attack cumulatively reach the armed attack threshold. In fact, it is more persuasive to reject the doctrine on its own terms with the argument that it 'undermines the temporal dimension of self-defence and risks turning a temporal right into an open-ended licence to use force'.[124]

Coming back to countermeasures, if so-called active defences are taken into account as possible actions to be taken and justified as countermeasures, further legal issues need to be considered. Active defences involve the employment of potentially harmful code aimed at the attacker, or even the plain 'mirroring' of malicious data back towards its source. As already pointed out by several authors, such action might lead to an uncontrollable threat of malicious code,[125] endangering previously uninvolved third parties. The ILC maintains the view that affecting third parties does not necessarily render a countermeasure unlawful. While it is clear that '[c]ountermeasures may not be directed against States other than the responsible State',[126] '[t]his does not mean that countermeasures may not incidentally affect the position of third States or indeed other third parties [...], as indirect or collateral effects cannot be entirely avoided'.[127] However, it has reasonably been suggested that whatever the circumstances of a given situation, a State which resorts to countermeasures is under an obligation to take every possible measure to avoid affecting third parties, or, if injury is inevitable, to ensure that the impact is kept to the minimum.[128] Yet, the question remains of how to define 'incidentally' in this context. More precisely, what degree of due diligence is required of the State that resorts to active defences as countermeasures against a cyber attack? At least in situations in which a defending State is aware of the fact that the active cyber defence cannot be designed in such a way as to not inevitably spread uncontrollably into the systems of innocent third parties, causing material loss, the response has to be considered unlawful *in relation to the third State*, triggering international responsibility

122 *Ibid*, 388.

123 ILC Articles, Commentaries, Article 30, at para. 3.

124 Tams, 2009, *op. cit.,* 389; a more thorough discussion of these issues regarding self-defence is beyond the scope of this chapter.

125 Roscini, *op. cit.,* 114; Hathaway *et al.*, *op. cit.,* 859.

126 ILC Articles, Commentaries, Article 49, at para. 4.

127 *Ibid.*, at para. 5.

128 Elagab, *op cit.*, 113.

towards it.[129] The same principle arguably applies when the incidental damage is merely foreseeable.

A similar issue emerges with regard to human rights. Article 50(1)(b) of the ILC Articles on State Responsibility explicitly stipulates that '[c]ountermeasures shall not affect obligations for the protection of fundamental human rights'. As countermeasures by definition concern State-to-State relations, the provision intends to prevent is an incidental, consequential impact on those human rights that are considered particularly important.[130] In order to clarify the norm, the ILC refers in its Commentaries to a General Comment by the Committee on Economic and Social Rights,[131] which in view of economic sanctions installed by international organisations stressed that '[i]n considering sanctions, it is essential to distinguish between the basic objective of applying political and economic pressure upon the governing élite of the country to persuade them to conform to international law, and the collateral infliction of suffering upon the most vulnerable groups within the targeted country',[132] and that 'whatever the circumstances, such sanctions should always take full account of the provisions of the International Covenant on Economic, Social and Cultural Rights'.[133]

The same rationale ought to be applied to the employment of countermeasures.[134] Thus, the provision intends to generally restrict the adoption of countermeasures that have the consequence of detrimentally affecting fundamental human rights, both intended and unintended.[135] Here, just as with the collateral impairment of the rights of third States, the determining rule can only be that a State which is resorting to countermeasures is under the obligation to respect human rights – especially those of the target State's civilian population – as far as possible.[136] Applied to the cyber context, the question is whether certain active defences can possibly be designed in such a way as to not automatically run the risk of seriously impairing those rights due to the very high probability of spreading uncontrollably. As noted by Hinkle,[137] at least simple mirroring of an ongoing DDoS attack can hardly be controlled in such a way as to minimise heavy risks for civilian infrastructure in the target country. As a consequence, it appears doubtful whether such conduct can ever meet the requirement of Article 50(1)(b). Caltagirone and Frincke

129 With the same conclusion also Hathaway *et al.*, *op cit.*, 859.

130 See Crawford, 2001, Introduction to the ILC Commentaries, Cambridge, 50.

131 ILC Articles, Commentaries, Article 50, at para. 7.

132 CESCR, General Comment 8, The relationship between economic sanctions and respect for economic, social and cultural rights, UN Doc E/C.12/1997/8, 12 December 1997, at para. 4.

133 *Ibid.*, at para. 1.

134 ILC Articles, Commentaries, Article 50, at para. 7.

135 Borelli/Olleson, 2010, Obligations Relating to Human Rights and Humanitarian Law, in Crawford *et al.* (ed.), *The Law of International Responsibility*, Oxford 2010, at 1177, 1182; also Sreenivasa Rao, 2004, Countermeasures in International Law. The Contribution of the International Law Commission, *in Studi di diritto internazionale in onore di Gaetano Arangio-Ruiz*, Napoli 2004, 853, 869 *et seq.*

136 Elagab, *op. cit.,* 100.

137 Hinkle, *op. cit.,* 21.

point to a particularly crucial issue when holding that '[t]here are real risks that the target of response might be a life, safety, or national security critical system, possibly of more value than the one under attack. A by-product of active response could be an increase of threat to critical systems, to be used as shields from active responses.'[138] In other words, there is a considerable danger that once the active cyber defence scheme is widely employed and known among adversaries, perpetrators might well be inclined to route attacks through sensitive systems in order to significantly increase the costs of otherwise likely lawful countermeasures.[139]

The third matter particularly critical as regards the employment of active defences as countermeasures is proportionality, mainly as a consequence of the same deliberation as outlined in connection to third States and human rights. Hinkle reasonably observes that while active defences are to be considered reciprocal countermeasures – thus in principle more easily satisfying the proportionality requirement according to the ILC[140] – 'there is no guarantee that these reciprocal tactics will produce a reciprocal effect'.[141] This is certainly true as regards pure numbers – a counterattack targeted at a larger network is likely to affect more computers. However, it has already been pointed out that quantitative deliberations do not suffice when assessing proportionality, as asserted by the arbitral tribunal in the *Air Services Agreement* case.[142] When taking into account qualitative considerations, disproportionate results might well occur when the employment of active defences hits critical or otherwise sensitive infrastructure in the target State, in a worst-case scenario even leading to civilian casualties.[143] However, while it appears correct to consider such an outcome as not meeting the proportionality requirement, it is also an obvious breach of Article 50(1)(b) of the ILC Articles on State Responsibility.[144] Such conduct cannot therefore be justified, and again suggests that there is a risk inherent in the very concept of active defences that hints at this possibility.

The issue of reversibility needs to be tackled briefly. Pursuant to Article 49(3) of the ILC Articles on State Responsibility, countermeasures must be executed in such a way as to 'permit the resumption of performance of the obligations in question', which amounts to an obligation to limit conduct to means that are reversible as far as possible. The underlying rationale is the concept of strict instrumentality of the remedy: countermeasures may only be invoked in order to achieve 'compliance by the target

138 Caltagirone/Frincke, *op. cit.*, 263.

139 Such a prospective tactic might even be likened to the use of so-called 'human shields' in armed conflicts; see e.g. Gross, 2002, Use of Civilians as Human Shields: What Legal and Moral Restrictions Pertain to a War Waged by a Democratic State Against Terrorism*?, Emory International Law Review,* 445.

140 ILC Articles, Commentaries, Part Three Chapter II, at 5.

141 Hinkle, *op. cit.,* 20.

142 Case Concerning the Air Services Agreement of 27 March 1946 (*United States of America v. France*), 9 December 1978, 18 RIAA 416, at para. 83.

143 See Hinkle, *op cit.*, 20.

144 See para. 3.1.2.

State with its international obligations of cessation and reparation',[145] which means that they can only be 'justified [...] insofar as they continue to be necessary to that end'.[146] When active cyber defences are employed against the source of the attack, this aspect could turn out to be critical. At least it seems to follow from the principle that the source must not be disabled permanently, and defenders would be under a legal duty to ensure that no damage is caused by the counterattack that cannot be reversed. Therefore, under the regime of countermeasures, 'highly aggressive measures intended to inflict the same kind of damage on the attacker that he or she is attempting to inflict on the victim',[147] or 'damaging the perpetrator's system to stop it from launching future attacks'[148] cannot be considered justifiable. Such intensive conduct might be justified in genuine situations of self-defence if all preconditions are met, but the requirement of reversibility would prevent a justification as a countermeasure. The Tallinn Manual seems to acknowledge this difficulty when asserting that 'actions involving the permanent disruption of cyber functions should not be undertaken in circumstances where their temporary disruption is technically feasible and would achieve the necessary effect'.[149] However, it is at least doubtful whether permanent damage could be legal at all, disregarding the question of the availability of less harmful means.

A different matter is the issue of loss of functionality triggered, for instance, by the unavailability of targeted systems during the counterattack. Crawford argued that 'whereas a measure may be reversible (assets can be unfrozen, civil aviation can be resumed) its effects while it was in force will rarely be entirely reversible, since consequential losses will have been suffered, by the target State and by third parties.'[150] Such losses are precisely envisaged with the notion that the effects of countermeasures should be reversible 'as far as possible'. Consequences of such a purely secondary nature – of course only as long as they are not disproportionate or in conflict with fundamental human rights – will not preclude the lawfulness of active defences as countermeasures, even if they turn out to be of a permanent nature.

It should be noted that this chapter focuses on the employment of active defences that are to be justified as countermeasures, because academic and political debate so far has mainly revolved around this issue. Of course, countermeasures can just as well assume an entirely different, more traditional shape, such as economic pressure or the suspension of a bilateral obligation in order to urge the other State to comply with

145 Crawford, Third Report on State Responsibility – Addendum 3, A/CN.4/507/Add.3, 18 July 2000, at para. 331.

146 *Ibid.*

147 Dittrich/Himma, 2005, Active Response to Computer Intrusions, in Bidgoli (ed.), *The Handbook of Information Security*, Hoboken, 664, 679.

148 Sklerov, *op. cit.,* 25.

149 Tallinn Manual, *op cit.*, Rule 9, para. 6.

150 Crawford, Third Report on State Responsibility – Addendum 3, A/CN.4/507/Add.3, 18 July 2000, at para. 330.

its duty to prevent cyber attacks. Arguably, this role of countermeasures in the cyber security context might even become the more prevalent one in the long run.

As with self-defence, countermeasures have the potential to play a role within the transnational cyber security framework. Some of the intricate and in fact insurmountable attribution issues are the same, while some may be avoided if the duty to prevent cyber attacks is taken into consideration. Compared to self-defence, non-forcible countermeasures arguably are less likely to entail a dangerous escalation of conflict. However, attempting to justify active cyber defences as countermeasures, as favoured by several scholars and practitioners, appears to be problematic on various grounds and, in the majority of cases, those legal restrictions will effectively prevent the lawful employment of this remedy. Therefore, countermeasures will most likely be more significant beyond considerations of pure instant protection against imminent or on-going cyber attacks. In particular, where a State demonstrably and continuously fails to abide by its obligations to prevent harm on other States, counter-measures other than active defences and cyber measures, could be used to enforce international law.

3.2 Necessity

If self-defence and countermeasures are both legally problematic as readily available unilateral remedies against cyber attacks due to the problems of sufficiently assured identification and thus attribution, what may also come into focus is the legal notion of necessity. Under such a situation, a State may invoke the existence of a state of emergency in order to undertake measures that otherwise would be unlawful. As a matter of principle, under such conditions the question is not who or what caused the situation, but only what is necessary in order to avert the danger or mitigate the harm caused by the situation. Thus, the issue of attribution is circumvented. Indeed, there need not be an intentionally harmful act in the first place: imminent hazard caused by altered or failing systems could just as well be an accidental consequence of entirely lawful conduct originating on another State's territory. The doctrine of necessity would be applicable in any case.

Although listed in the same section of the ILC Articles on State Responsibility as self-defence and countermeasures as one of the 'circumstances precluding wrongfulness', necessity is structurally different and in fact hardly at all comparable with the other two. The two concepts analysed above are remedies in the strict sense, also serving the purpose of enforcing international law that transcends the mere function of justification of otherwise internationally wrongful conduct. For self-defence, this is at least true to some degree; for countermeasures, this aspect is one of the central features and thus generally acknowledged. To 'resort' to necessity can only mean to invoke a truly exceptional circumstance that in this very specific factual situation may be considered sufficiently significant that the conduct in question will, by way of absolute exception, not be deemed a violation of international law triggering the acting State's responsibility.

Necessity, at least as envisaged by Article 25 of the ILC Articles on State Responsibility, is thus hardly a legal 'tool' suitable for serving as a strategy to counter cyber threats. In fact, necessity is considered so different that some commentators during the Articles' drafting process suggested that necessity could merely act as an 'excuse', but not as a 'justification' of wrongful conduct, even if the outcome in both instances is the absence of responsibility.[151]

Still, it seems worthwhile to analyse the preconditions of Article 25 with respect to cyber attacks in order to assess whether and if so, to what *a priori* limited degree necessity could play a role within the cyber security framework. More precisely, if the employment of active defences is technically and politically considered to be a useful tool against cyber attacks, the question arises whether such intrusive measures – that at least *prima facie* would seem to violate the customary principle of non-intervention – could be justified under Article 25 in situations where sufficient identification of the author is unobtainable.

Although controversial during the drafting process[152] and occasionally still called into question,[153] today it is generally acknowledged that Article 25 of the ILC Articles on State Responsibility reflects customary international law.[154] According to the text of the norm:

> [n]ecessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act is the only way for the State to safeguard an essential interest against a grave and imminent peril, and does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community a whole. In any case, necessity may not be

151 See most prominently Lowe, 1999, Precluding Wrongfulness or Responsibility: A Plea for Excuses, 10 *European Journal of International Law* 405; Romano, 1999, Combating Terrorism and Weapons of Mass Destruction: Reviving the Doctrine of a State of Necessity, 87 *Georgetown Law Journal* 1023, 1046 *et seq.*; Tsagourias, 2010, Necessity and the Use of Force: A Special Regime, 41 *Netherlands Yearbook of International Law* 11, 39 *et seq.*; Simma, 1986, *op. cit.,* 357, 381 *et seq.* (1986).

152 See the comment by the United Kingdom, A/CN.4/488, 25 March 1998, at para. 88.

153 See especially Sloane, 2012, On the Use and Abuse of Necessity in the Law of State Responsibility, 106 *American Journal of International Law* 447, 450 *et seq.*; Kurtz, 2010, Adjudging the Exceptional at International Investment Law: Security, Public Order and Financial Crisis, 59 *International and Comparative Law Quarterly* 325, 344; Brownlie, 2008, *Principles of Public International Law*, 7th edition, Oxford, at 466; *New Zealand v France* [1990] 20 RIAA 215, 254.

154 ICJ, *Gabcikovo-Nagymaros Project*, at para. 51; ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, at para. 140; ICSID, *Sempra Energy International v. Argentine Republic*, ARB/02/16, 28 September 2007, at para. 378; ICSID, *Continental Casualty Company v. Argentine Republic*, ARB/03/9, 5 September 2008, at para. 165; *The M/V 'Saiga' (No. 2) Case (Saint Vincent and the Grenadines v. Guinea)*, [1999] International Tribunal for the Law of the Sea (ITLOS), paras. 133-34; for an example on the national level see the German Federal Constitutional Court, BVerfG, 2 BvM 1/03, 8 May 2007, at para. 36, based on Reinisch, 2008, Sachverständigengutachten zur Frage des Bestehens und der Wirkung des völkerrechtlichen Rechtfertigungsgrundes 'Staatsnotstand', 68 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 4, 5-10.

> invoked by a State as a ground for precluding wrongfulness if the international obligation in question excludes the possibility of invoking necessity, or the State has contributed to the situation of necessity.

The negative phrasing unambiguously indicates that necessity may only be invoked in absolutely exceptional circumstances. The main reason for this caution on the part of the ILC is a history of severe abuses of the doctrine.[155] The requirements for an invocation to be accepted are accordingly strict. First, an 'essential interest' must be at stake, which must be in 'grave and imminent peril'. Which interests may be considered essential cannot be predetermined; however, international practice shows a wide range of concerns, for instance the environment,[156] grave difficulties as regards a State's financial obligations,[157] and the protection of a State's civilian population from terrorist attack.[158] Translated to the cyber context, it seems reasonable to assume that at least the protection of critical infrastructure would be accepted as such an essential interest, and recent statements by various States and international organisations point into that direction. Defined as 'structures and functions which are indispensable for the vital functions of society',[159] virtually all national cyber security strategy papers underline the protection of critical infrastructure as one of the principal goals of any cyber security efforts.[160] Accordingly, the Tallinn Manual directly links those assets to the notion of a situation of necessity by asserting that 'if faced with significant cyber operations against a State's critical infrastructure, the plea of necessity could justify a State's resort to counter-hacking'.[161] Therefore, the qualification of critical infrastructure as an essential interest appears sufficiently verified.

---

155 Heathcote, 2010, Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Necessity, in Crawford *et al.* (ed.), *The Law of International Responsibility*, Oxford, at 492.

156 See only ICJ, *Gabcikovo-Nagymaros Project*, *op. cit*.

157 See the ICSID and BVerfG, *op. cit.*; for an analysis see Bjorklund, 2008, Emergency Exceptions: State of Necessity and Force Majeure, in Muchlinski *et al.* (ed.), *The Oxford Handbook of International Investment Law*, Oxford, 459, 481.

158 ICJ, *Wall* advisory opinion, at para. 140; the reason why necessity was rejected was the argument that 'the Court [was] not convinced that the construction of the wall along the route chosen was the only means to safeguard the interests of Israel against the peril which it has invoked as justification for that construction', which implies the acknowledgment of the population's security as an essential interest, however, see Tams, 2005, Light Treatment of a Complex Problem: The Law of Self-Defence in the Wall Case, *16 European Journal of International Law* 963, 967, noting that the Court was 'cautiously avoiding any general position on the availability of necessity'.

159 Thus for instance Finland's Cyber Security Strategy, January 2013, available at: http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, at 12.

160 The UK Cyber Security Strategy, November 2011, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, at 8; U.S. Department of Defense Strategy for Operating in Cyberspace, July 2011, available at: http://www.defense.gov/news/d20110714cyber.pdf, at 4; Stratégie de la France, Défense et sécurité des systèmes d'information, 2011, available at: http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011, at 7 ('infrastructures vitales nationales'); Cyber-Sicherheitsstrategie für Deutschland, February 2011, available at: at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, at 6.

161 Tallinn Manual, *op cit.*, Rule 9, para. 12.

The essential interest must be threatened by a grave and imminent peril. While the State is not required for to prove that the peril 'would certainly have occurred',[162] it needs to be 'objectively established and not merely apprehended as possible'.[163] This matter is of course essentially context-specific. As for imminence, it seems beyond doubt that at least an ongoing cyber attack such as a persistent DDoS attack which targets critical infrastructure would satisfy the requirement. At the other end of the spectrum, once an attack has definitely come to an end, a situation of necessity no longer exists.[164] In this sense, the so-called 'accumulation of events' doctrine occasionally invoked in order to justify unilateral measures of self-defence in reaction to a number of small-scale attacks each not reaching the armed attack threshold is not applicable *per se* to the context of necessity.[165] As noted by Laursen, '[t]he necessity response is an emergency response to deal with the immediate grave peril at hand, not the five previous attacks during the past six months in addition to the imminent attack'.[166]

Apart from such clear cases, the technical peculiarities of cyberspace may make it enormously difficult in certain situations to determine whether a threat looms that is already sufficiently imminent for a certain action to be justified under necessity. For instance, does the detection of a security breach in a critical system warrant active defensive measures directed against the purported source of the cyber operation? Note once again that it might be almost impossible to establish whether the infiltration of alien code was carried out for espionage or destructive purposes.[167] In case of the former, there may arguably be no peril within the meaning of Article 25 at all. In case of the latter, the security breach might even be the penultimate step before the launching of a final, potentially disastrous attack.[168] Such a situation is not characterised by 'uncertainty' as envisaged by Crawford, which, if at hand, should not 'disqualify a State from invoking necessity',[169] but by 'indeterminacy', as argued by Foster, due to

162 Crawford, Second Report on State Responsibility – Addendum 2, A/CN.4/498/Add.2, 30 April 1999, at para. 289.

163 ILC Articles, Commentaries, Article 25, at para. 15.

164 See ICJ, *Gabcikovo-Nagymaros Project*, *op. cit.,* at para. 55: 'The Court would however point out that the bed of the Danube in the vicinity of Szentendre had already been deepened prior to 1980 in order to extract building materials, and that the river had from that time attained, in that sector, the depth required by the 1977 Treaty. The peril invoked by Hungary had thus already materialised to a large extent for a number of years [...]'.

165 See on that doctrine Tams, 2009, The Use of Force Against Terrorists, 20 *European Journal of International Law* 359, 370 and 388.

166 Laursen, 2004, The Use of Force and (the State of) Necessity, 37 *Vanderbilt Journal of Transnational Law* 485, 522.

167 Melnitzky, *op cit.*, 565 *et seq.*; Lin, *op cit.*, 78.

168 Take as an example the recently detected intrusions into U.S. critical infrastructure systems; see Perlroth/Sanger, 2013, New Computer Attacks Traced to Iran, Officials Say, *The New York Times*, 25 May, p. A10: The cyber operations allegedly 'were devised to destroy data and manipulate the machinery that operates critical control systems of U.S. critical infrastructure, like oil pipelines. One official described them as '*probes that suggest someone is looking at how to take control of these systems*'.' (emphasis added).

169 Crawford, Second Report on State Responsibility – Addendum 2, A/CN.4/498/Add.2, 30 April 1999, at para. 289.

the fact that it is still an individual who must decide to carry out the final step in order to trigger the damaging event: 'Future human behaviour is commonly indeterminate', which is why '[t]he indeterminacy of [human] actions might preclude the application of the doctrine of necessity'.[170] This conclusion was also implied by the ICJ in its decision on the *Gabcikovo-Nagymaros Project*.[171] Following this line of argument, unless the initial infiltration implemented a 'logic bomb' – which is triggered without further human intervention once certain determining conditions are met – even potentially damaging code would not pose an imminent peril. With regard to self-defence, faced with a corresponding issue the majority of the International Group of Experts at Tallinn argued that the deciding factor should be the so-called 'last feasible window of opportunity',[172] meaning that 'an armed attack becomes imminent at the point that the victim State must act lest it lose the opportunity to defend itself effectively'.[173] Foster suggests a similar approach concerning necessity, holding that the bottom line should be that 'harm becomes "imminent" at the point when it appears reasonable for a State invoking necessity to conclude [...] that preventive action must be taken'.[174] As asserted by Crawford, the required standard in this sense can only be the 'evidence reasonably available at the time' of the assessment.[175] Thus, factual error would be excused as long as the decision to act was made with due care,[176] which means that the necessity doctrine in this respect operates critically different from both self-defence and countermeasures.

Still, this rationale will not easily be transferred to cyber attack scenarios. The deliberately narrow scope of Article 25 of the Articles on State Responsibility, establishing necessity as an absolute exception, calls for a cautious approach, which means that in the determination of an imminent peril the requirement of due care needs to be taken seriously. In case of doubt, the rule-exception relationship should necessitate that no action be taken. While this conclusion might come across as being far from satisfactory for policy makers, it is a direct consequence of the deliberately narrow scope of the application of necessity. Necessity is only to be invoked in most exceptional circumstances; it is not a substitute for self-defence or countermeasures in cases in which their legal requirements are not fulfilled; rather, as a general rule where the conditions of either self-defence or countermeasures are not met, no unilateral (unlawful) action may be taken and only exceptionally will it be the case that such conduct could be justified on the basis of necessity.

---

170 Foster, 2008, Necessity and Precaution in International Law: Responding to Oblique Forms of Urgency, 23 *New Zealand Universities Law Review* 265, 282.

171 ICJ, *Gabcikovo-Nagymaros Project*, *op. cit.,* at para. 55.

172 Tallinn Manual, *op cit.*, Rule 15, at para. 4.

173 *Ibid.*, at para. 6.

174 Foster, 2008, *op. cit.*, 277.

175 Crawford, Second Report on State Responsibility – Addendum 2, A/CN.4/498/Add.2, 30 April 1999, at para. 289.

176 Likewise Krieger, *op. cit.,* 16.

In any case, for it to be justified under the doctrine of necessity, the measure chosen to avert the grave and imminent peril must be the only one available. The case law of international courts and tribunals confirms that it is here where most invocations of the principle ultimately fail.[177] This outcome is logically stringent: as long as there are alternatives, a particular measure is not *necessary* in the strict sense of the term. However, the application of the test has been so strict that it provoked commentators to call it 'essentially meaningless'.[178] Of course, it will frequently be impossible to show counterfactually whether other means would in fact have been available, and this must hold even more true when it comes to cyber security matters. Thus, the only thing that seems entirely clear is that the employment of active defences can only ever be taken into consideration as a last resort. As long as there are other, none-intrusive means available which are sufficient to end the effects of a cyber attack, the invocation of necessity in order to justify active cyber defences is precluded, even if those are more expensive or less convenient to use.

Pursuant to Article 25, besides the preconditions already mentioned, the measure taken must not seriously impair an essential interest of another State, and the acting State is precluded from invoking necessity when it has contributed to the situation of necessity. Finally, reliance on necessity is legally impossible if the international obligation in question excludes this particular justification. As for the question of contribution, the ILC only asserts that its impact on 'the situation of necessity must be sufficiently substantial and not merely incidental or peripheral'.[179] This is a matter which is hardly specific to the cyber security context. Of course one may ask for instance whether Estonia 'contributed' to the persistent DDoS attacks against it in 2007 when it 'provoked' Russia and its own Russian minority by moving the Soviet monument. Apart from the consideration that the answer to this question can only rationally be that such a kind of contribution that stems from a wholly legal act undertaken within its own *domaine réservé* cannot preclude a State from invoking necessity when facing a subsequent peril, the example shows that a lot of these issues will concern scenarios situated outside the strict cyber realm. A different matter would be whether one might reasonably argue that a negligently insecure cyber infrastructure which is excessively prone to security breaches might count as a contribution to a hazardous situation in the sense of the norm.

The question of the other States' essential interests or those of the international community as a whole is probably more critical in view of the possibility to employ

177 See e.g. ICJ, *Wall* advisory opinion, at para. 140; ITLOS, The M/V 'Saiga' (No. 2) Case (*Saint Vincent and the Grenadines v. Guinea*), 1 July 1999, at para. 134; ICSID, CMS *Gas Transmission Company v. Argentine Republic*, ARB/01/8, 12 May 2005, at para.323 *et seq.*; ICSID, *Sempra Energy International v. Argentine Republic*, ARB/02/16, 28 September 2007, at para. 350; ICSID, *Continental Casualty Company v. Argentine Republic*, ARB/03/9, 5 September 2008, at para. 221 *et seq.*

178 Waibel, 2007, Two Worlds of Necessity in ICSID Arbitration: CMS and LG&E, 20 *Leiden Journal of International Law* 637, 646; similarly Kurtz, *op cit.*, 342.

179 ILC Articles, Commentaries, Article 25, at para. 20.

active defences, as envisaged *inter alia* by the Tallinn Manual. Active cyber defence measures are inherently dangerous, posing the risk of at least incidentally hitting critical cyber infrastructure within the target State. Within the context of necessity, this observation is even more significant, as the latter State's responsibility for the initial attack against the victim State is not relevant for the legal assessment of the measure. Regarding the relevant standard, the ILC rather bluntly asserts that 'the interest relied on must outweigh all other considerations, not merely from the point of view of the acting State but on a reasonable assessment of the competing interests'.[180] This is another deliberately high threshold, erected in order to make reliance on necessity as rarely available as possible. Arguably, in many scenarios it would follow from this that no permanent damage or obstruction of network functionality may ever be inflicted on the target State's systems under the doctrine of necessity. In order to 'outweigh all other considerations' 'on a reasonable assessment of the competing interests', only a temporary interruption to stop a malicious signal or data flow from causing further damage within the victim State's own systems may be justifiable. Only if a certain active defence measure by way of 'counter hacking' into the alleged adversary's systems is capable of ensuring that no further, persistent harm is done, such measure can be a legally valid tool under the concept.

Further than the clearly limiting but not absolute statement in the commentary to the Tallinn Manual, according to which '[w]hether a State may use force in accordance with the plea of necessity is highly uncertain',[181] forcible measures can never be justified on the basis of the necessity doctrine.[182] The permission for the use of force, at least if it does not amount to an act of 'aggression',[183] under the necessity doctrine has been suggested in the recent past, mostly in connection with humanitarian interventions and counter-terrorism.[184] A detailed discussion of this issue is beyond the scope of this chapter. However, even if one does not accept that the prohibition of the use of force as such is a peremptory norm of international law,[185] which would mean that it would not

180 *Ibid.*, at para. 17.

181 Tallinn Manual, *op cit.*, 39.

182 *Ibid.*

183 See Definition of Aggression, GA/Res 3314 (XXIX), 14 December 1974.

184 See already Ago, Eighth Report on State Responsibility. Addendum: The internationally wrongful act of the State, source of international responsibility (part I) (concluded), A/CN.4/318/ADD.5-7, 1980, at para. 59 *et seq.*; Crawford, Second Report on State Responsibility - Addendum 2, A/CN.4/498/Add.2, 30 April 1999, at para. 287; Gazzini, *op cit.*, 206 *et seq.*; Johnstone, 2005, The Plea of 'Necessity' in International Legal Discourse: Humanitarian Intervention and Counter-Terrorism, 43 *Columbia Journal of Transnational Law* 337; Laursen, *op cit.*, 485; Romano, 1999, Combating Terrorism and Weapons of Mass Destruction: Reviving the Doctrine of a State of Necessity, 87 *Georgetown Law Journal* 1023; but see Corten, 2004, Létat de nécessité peut-il justifier un recours à la force non constitutif d'agression?, 4 *The Global Community Yearbook of International Law & Jurisprudence* 11.

185 For an analysis see Green, 2011, Questioning the Peremptory Status of the Prohibition of the Use of Force, 32 *Michigan Journal of International Law* 215; Koskenniemi, 2006, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law. Report of the Study Group of the International Law Commission, A/CN.4/L.682, 13 April 2006, at para. 374: 'Overall, the most frequently

already be precluded by way of Article 26 of the ILC Articles on State Responsibility, it seems reasonable to conclude that a forceful protective reaction would inevitably 'seriously impair the essential interest[s] of the target State concerning respect for its territorial integrity'.[186] Furthermore, and even more strikingly, it might be argued that the UN Charter sets up a legal regime concerning legal uses of force that implicitly excludes the invocation of necessity pursuant to Article 25(2)(a) of the ILC Articles on State Responsibility.[187]

Ultimately, the analysis of necessity in view of cyber security leaves a mixed impression at best. While the issue of identification and attribution is circumvented, the preconditions of Article 25 are intentionally strict to such a degree that it is highly doubtful whether the necessity defence will be available in more than a very few exceptional and rather hypothetical cases that are characterised by very specific circumstances. On the other hand, precisely because attribution is no requirement, the doctrine opens the possibility of serious abuse, an observation that is even more relevant if one takes into consideration that there is a persistent tendency to attempt to justify even the use of force by way of invoking necessity.

The general customary defence of necessity as described by Article 25 is by and large not a useful tool within the cyber security context. Notwithstanding this conclusion, and in view of persistent and arguably insurmountable attribution problems, a treaty-based special necessity regime that is tailor-made for specific problems encountered in the cyber context should not be discarded out of hand. Special necessity norms are common in the international plane, either as emergency exceptions within treaties,[188] or as a standalone body of rules concerned with a particular subject. The relationship between the general necessity provision of Article 25 of the ILC Articles on State Responsibility and the special norms is governed by Article 55 of the ILC Articles on State Responsibility, which provides that '[t]hese articles do not apply where and to the extent that the conditions for the existence of an internationally wrongful act or the content or implementation of the international responsibility of a State are governed by special rules of international law' – in other words, the latter are *lex specialis*. The most frequently cited example for a standalone regime, even if only rarely – if ever – actually

cited candidates for the status of *jus cogens* include: (a) **the prohibition of** *aggressive* **use of force**; […]' (emphasis added); ILC Commentaries, Article 26, at para. 5.

186 Thus expressly Rytter, 2001, Humanitarian Intervention without the Security Council: From San Francisco to Kosovo – and Beyond, 70 *Nordic Journal of International Law* 121, 134 *et seq.*.

187 Corten, *op cit.*, 48: 'Une interprétation du texte de la Charte, tel qu'il a été conçu puis interprété par le biais de plusieurs résolutions adoptées par l'Assemblée générale, confirme que la prohibition du recours à la force représente un régime juridique *qui n'admet pas d'échappatoire*.' (emphasis added).

188 Sloane, *op cit.*, 454, suggests that the number of such provisions must be 'hundreds'; see e.g. Article 4(1) ICCPR; Article 15(1) ECHR; Article 27(1) ACHR; Article XXI(b)(iii) GATT; Article XI of the 1991 *Treaty Between United States of America and the Argentine Republic Concerning the Reciprocal Encouragement and Protection of Investment*; Article XX(1)(d) of the 1955 *Treaty of Amity, Economic Relations, and Consular Rights Between the United States of America and Iran*; Article 221(1) UNCLOS.

invoked by a State,[189] is the 1969 *International Convention Relating to Intervention on the High Seas in Cases of Oil Pollution Casualties* (Intervention Convention). Drafted and agreed upon after the disastrous *Torrey Canyon* oil tanker accident off the Cornish coast in 1967.[190] Although the bombing of the wrecked Liberian-registered tanker by the United Kingdom in order to burn the spilling oil and prevent it from reaching the coast was not justified in legal terms, the action was cited early on as one example for the existence of a customary law defence of necessity.[191] Even though it was not met with legal resistance by other States,[192] in the aftermath of the incident it was quickly deemed necessary to come up with a specific multilateral convention that outlines the exact preconditions and legal consequences of such emergency actions on the high seas, as 'States preferred to establish clear international law on the legal issues arising out of such accidental spills rather than to leave comparable future incidents to the unilateral judgments of affected States'.[193]

Without going into detail as regards the exact content of such a legal regime, it is likely that the Intervention Convention may provide a model for a parallel treaty that would govern States' reactions to future hazardous cyber incidents. The more that States and modern societies become reliant on a functioning and unimpeded cyberspace, the more likely it is that cyber incidents, whether accidental or inflicted intentionally, will affect a State's 'essential interests'. Moreover, in the interconnected domain of cyberspace it appears rather likely that a quick-fix solution to the problem that helps to safeguard the interests of one State might affect the interests of another; temporarily degrading cyber traffic to protect one's own systems may affect the systems and/or interests of other States. A treaty specifically focused on large-scale cyber incidents could help to resolve the legal uncertainties resulting from the application of the necessity doctrine in the cyber domain and at the same time help to confine the various risks and incalculability pertaining to the application of the general necessity norm of Article 25.

189 Wendel, 2007, *State Responsibility for Interferences with the Freedom of Navigation in Public International Law*, Heidelberg, at 49.

190 See BBC News, On This Day: 1967: Supertanker Torrey Canyon hits rocks, available at: http://news.bbc.co.uk/onthisday/hi/dates/stories/march/18/newsid_4242000/4242709.stm.

191 See Ago, Eighth Report on State Responsibility. Addendum: The internationally wrongful act of the State, source of international responsibility (part I) (concluded), A/CN.4/318/ADD.5-7, 1980, at para. 35; Utton, 1968, Protective Measures and the 'Torrey Canyon', 9 *Boston College Industrial and Commercial Law Review* 613, 624 *et seq.*; ILC Articles, Commentaries, Article 25, at para. 9.

192 However, Wendel, *op cit.*, 97, reports that '[t]he United States submitted a working paper which clearly outlined that no authority exists to take action on the high seas'; Emanuelli, 1976, The Right of Intervention of Coastal States on the High Seas in Cases of Pollution Casualties, 25 U.N.B. *Law Journal* 79, 87, reports that the right to bomb the ship invoked by the UK government 'was denied by some organisations like the British Chamber of Shipping'.

193 Sloane, *op. cit.*, 468.

4. In Search of a More Comprehensive Approach: Spelling Out States' Due Diligence Obligations in Cyberspace

So far, the focus of this chapter has been on unilateral protective remedies, invoked by States when faced with an emergency situation caused by a cyber incident. In order to reach a more general state of transnational security in cyberspace, such unilateral measures, though important in their own right, hardly suffice. What is needed at least in the midterm is a more comprehensive approach that complements those remedies, providing a legal framework that spells out the duties of States concerning cyber security more concretely. To be able to phrase such duties, it is necessary to inquire into the precise content of States' due diligence obligations regarding cyberspace, as already hinted at above.[194] As confirmed by the ICJ, 'the obligation to [prevent] is an obligation to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party'.[195] In other words, due diligence serves as the standard for any international duties to prevent certain events from occurring. It is an obligation of conduct, not of result.[196] Such standard is necessarily dependant on the context and must therefore be determined for every subject matter specifically, or may even change over time 'in light [...] of new scientific or technological knowledge', as argued by the International Tribunal for the Law of the Sea (ITLOS) in its 2011 advisory opinion.[197] As regards cyberspace, those obligations can hardly be considered settled.[198] Due diligence is generally understood to require conduct that would be adopted by any reasonable State under the given circumstances.[199] In relation to cyberspace and in view of the relative novelty of this domain (especially as a subject for discussion among States), however, it is often still not fully clear what exactly a reasonable State would do with respect to cyber security. However, analysing more general concepts of due diligence in international law, it may be possible to infer at least some guiding principles to be applied to the cyber security context.

---

194 See para. 3.1.2.

195 ICJ, *Case Concerning Pulp Mills on the River Uruguay* (*Argentine v Uruguay*), Judgment of 20 April 2010, at para. 197; see also at para. 223: '[T]he Court observes that the obligation to prevent [...], and the exercise of due diligence *implied in it*, [...]' (emphasis added).

196 ICJ, *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina v. Serbia and Montenegro*), Judgment of 26 February 2007, at para. 430.

197 ITLOS, *Seabed Disputes Chamber, Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion of 1 February 2011, at para. 117.

198 For analyses on other subject matters see e.g. Barnidge, *op cit*., 103; Crimm, 2005, Post-September 11 Fortified Anti-Terrorism Measures Compel Heightened Due Diligence, 25 *Pace Law Review* 203 (2005); Dupuy/Hoss, 2006, Trail Smelter and Terrorism: International Mechanisms to Combat Transboundary Harm, in Bratspies & Miller (eds.), *Transboundary Harm in International Law. Lessons from the Trail Smelter Arbitration*, Cambridge 2006, p. 225; Heathcote, 2012, State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility, in Bannelier *et al.* (eds.), *The ICJ and the Evolution of International Law. The Enduring Impact of the Corfu Channel Case*, London, 295.

199 Koivurova, 2012, Due Diligence, in Wolfrum (ed.), *The Max Planck Encyclopedia of Public International Law*, Oxford University Press.

As a consequence of the advent of transnational terrorism, the UN main bodies have adopted resolutions that can be read as catalogues of due diligence obligations to combat the threat, most significantly urging States to criminalise and prosecute terrorist acts, to cooperate to this end and more generally to exchange crucial information and not to (consciously) let their own territory become a launching base for terrorist attacks.[200] As those duties can by now be considered firmly established, it seems reasonable to assume that obligations concerning cyber security incidents will run along similar lines. As early as 2000, the UN General Assembly asked States to ensure that 'their laws and practice eliminate safe havens for those who criminally misuse information technologies'.[201] Shortly afterwards, the 2001 *Convention on Cybercrime*, initiated by the Council of Europe but open to non-Member States,[202] required signatory States to undertake measures of prevention by establishing 'criminal offences for almost every conceivable type of cyber-attack under their domestic laws'.[203] Thus, it may be argued that the due diligence standard at least amounts to the obligation to enact laws that criminalise cyber attacks, and to prosecute the perpetrators when an attack has occurred.[204] Directly alluding to earlier ICJ decisions and State practice concerning terrorism, the Tallinn Manual asserts that '[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States'.[205]

The duty to criminalise, which ideally amounts to prevention by deterrence, is necessarily complemented by a more general obligation of vigilance. In this sense, the ICJ held that due diligence

> is an obligation which entails not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement and the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party.[206]

While the general principle is certainly defendable, the question is what exactly this means for the cyber context. The Tallinn Group of Experts could not agree whether such a preventative duty exists as regards cyber attacks due to the inherent 'difficulty

200 See most significantly UN GA Res. 49/60 (9 December 1994); UN SC Res. 1267 (15 October 1999); UN SC Res. 1333 (19 December 2000); UN SC Res. 1368 (12 September 2001); UN SC Res. 1373 (28 September 2001).

201 UN GA Res. 55/63 (4 December 2000).

202 Council of Europe, *Convention on Cybercrime*, CET 185, signed 23 November 2001, effective 1 July 2004.

203 Sklerov, *op. cit.,* note 382 and accompanying text; see *Convention on Cybercrime*, Chapter II, Section 1, Articles 2 to 13.

204 Sklerov, *op. cit.,* 12; Kulesza, 2009, State Responsibility for Cyber-Attacks on International Peace and Security, 29 *Polish Yearbook of International Law* 139, 141.

205 Tallinn Manual, *op cit.*, 26.

206 ICJ, *Case Concerning Pulp Mills on the River Uruguay* (*Argentine v. Uruguay*), Judgment of 20 April 2010, at para. 197.

of mounting comprehensive and effective defences against all possible threats'.[207] In any case the due diligence standard would not impose an absolute obligation to avoid all attacks and there might thus still be cases – especially when continuous and/or similar attack patterns are at issue – where the State 'should have known' of malicious conduct within the networks on its own territory. In its *Corfu Channel* decision, the ICJ considered such constructive knowledge sufficient for a due diligence violation under certain factual conditions.[208] While cyberspace certainly is no waterway that is 'easily watched' [209] and while any potential due diligence obligation would have to be in line with international human rights obligations and not be used as a pretext for censorship and surveillance,[210] there are nonetheless scenarios imaginable where a State could have gained information about an imminent or continuously on-going attack, and it thus seems untenable to *a priori* exclude the possibility of assuming a due diligence obligation of vigilance towards cyber security incidents. The current problem is the determination of the 'threshold of due care' in this regard,[211] but, in line with the holding of ITLOS, the obligations in this regard could well be altered by new technological developments in the relevant field of cyber security.

Closely connected with this, several commentators have suggested that the due diligence obligations should encompass an element of precaution.[212] In other contexts it has been observed that precaution is an integral part of due diligence.[213] For the cyber context, Krieger suggests *inter alia* that precaution should comprise an obligation on all States and stakeholders to ensure that all relevant systems are always kept up to date in order for cyber security to work properly.[214] A corresponding duty has been implied by the ICJ in its *Pulp Mills* judgment in relation to the safe operation of an industrial plant.[215] Furthermore, it appears reasonable to assert that multilateral communication about possible technical failures and security-relevant shortcomings as well as other minor cyber incidents (especially when due to zero-day exploits) should be permanent and mandatory, in order to enable all States to prepare for possible attacks or security

207 Tallinn Manual, *op cit.*, 27.

208 ICJ, *The Corfu Channel Case* (*United Kingdom v Albania*) (Merits), Judgment of 9 April 1949, at 22: '[...] the laying of the minefield [...] could not have been accomplished without the knowledge of the Albanian Government'.

209 *Ibid.*, at 20.

210 See the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue by UN Special Rapporteur Frank La Rue A/HRC/23/40, 17 April 2013.

211 Tallinn Manual, *op cit.*, 28.

212 See generally Schröder, 2012, Precautionary Approach/Principle, in Wolfrum (ed.), *The Max Planck Encyclopaedia of Public International Law*, Oxford University Press.

213 ITLOS, Seabed Disputes Chamber, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion of 1 February 2011, at paras. 132-135.

214 Krieger, *op. cit.,* 19.

215 ICJ, *Case Concerning Pulp Mills on the River Uruguay* (*Argentine v. Uruguay*), Judgment of 20 April 2010, para. 223.

breaches.[216] Concerning both points, recent domestic legislative initiatives point in this direction, attempting to establish the legal duty on relevant enterprises to frequently update their systems to the latest security standards and to report cyber incidents in order to establish such a dialogue.[217]

In the case of an actual cyber security incident, such as a cyber attack or technical failure of critical cyber infrastructure, the content of due diligence obligations shifts, or rather is expanded. In such a situation, it seems reasonable to assert that the standard implies obligations to cooperate with the victim State in order to prevent further harm or to mitigate the consequences of an incident.[218] As already mentioned in the context of transnational terrorism, such duties of cooperation have long been acknowledged as an essential part of the due diligence principle. For instance, Article 4 of the ILC *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities* provides that 'States concerned shall cooperate in good faith [...] in preventing significant transboundary harm or at any event in minimizing the risk thereof'. Similarly, Article 6(1) of the World Health Organization's 2005 *International Health Regulations* obliges Member States to notify the organisation 'of all events which may constitute a public health emergency of international concern within [their territories]'. A duty of this kind could well be translated to the cyber security context, triggered by the event of an incident.[219] This approach, which primarily aims at prevention rather than repression, is not a panacea for cyber security but is an important stepping stone towards a more comprehensive approach to global cyber security and geo-cyber stability. In a domain where attribution of conduct is inherently difficult if not impossible, a much stronger focus should be placed on the preventive dimension than the repressive dimension, which is borrowed from military responses and the use of force. Establishing due diligence obligations on States to harden their systems and to criminalise data theft and system intrusions as well as other relevant conduct will not help to avert and prevent highly elaborate destructive attacks by powerful actors. It will, however, help to mitigate those

216 Krieger, *op. cit.,* 19; for the corresponding aspect in relation to environmental law and precaution see Foster, 2011, *Science and the Precautionary Principle in International Courts and Tribunals*, Cambridge, p. 35: '[...] working towards achieving the right balance between development and environmental protection has in general required the international community to focus on international cooperation rather than on State responsibility'.

217 European Union, *EU Cybersecurity Plan to protect open internet and online freedom and opportunity*, press release IP/13/94, 7 February 2013, available at: http://europa.eu/rapid/press-release_IP-13-94_en.htm; for Germany, *Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme*, 7 March 2013, available at: http://bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.html; the latter proposition by the Federal Ministry of the Interior however has met fierce opposition on the part of the concerned enterprises, see Cyberangriffe: Hacker-Meldepflicht für Unterehmen offenbar vor dem Aus, *Spiegel* [online], 5 June 2013, available at: http://www.spiegel.de/netzwelt/netzpolitik/hacker-meldepflicht-fuer-unternehmen-offenbar-vor-dem-aus-a-903824.html.

218 Kulesza, *op. cit.,* 149.

219 In this sense it might be said that, in 2007, Russia violated its due diligence obligation towards Estonia when it failed to cooperate to mitigate or obstruct the ongoing DDoS attacks emanating from its territory despite formal requests by Estonian authorities; see Evron, 2008, Battling Botnets and Online Mobs, *Georgetown Journal of International Affairs* 121, 124.

threats which make up the vast majority of contemporary threats and – once established and accepted – will make it harder for States that sponsor such activities to blame other actors. At the same time it must be acknowledged that setting up more elaborate and specific due diligence obligations will take time. Domestic legislative approaches towards information sharing and regular security updates, have stirred significant controversy due to the economic costs attached and the fact that information sharing in a security-sensitive area is inherently difficult to achieve. On the inter-State level these problems will certainly be no less relevant.

5. Conclusion

For the time being and also likely into the mid-term, with no comprehensive international cyber security treaty or centralised and institutionalised regime-building in sight,[220] unilateral remedies will most likely continue to play a central role when it comes to cyber security incidents. Thus far the academic and political debate has focused too much on military responses to cyber attacks, over-emphasising the self-defence doctrine as the most feasible reaction to malicious inter-State activity. This overemphasis is not only dangerous but also out of touch with reality and the kind of security threats States and societies actually face in cyberspace. To date no cyber security incident has actually risen to the level of an armed attack. Moreover, due to the persisting attribution problem and the myriad uncertainties surrounding tracing the origin of an attack in cyberspace, in most instances it will be legally untenable. In cyberspace, as in the real world, self-defence is an option of last resort.

This chapter has attempted to present and analyse alternatives to the military paradigm of cyber security. It has been made clear that both countermeasures and the state of necessity pose unique and very specific legal problems when applied in the context of cyberspace. Some of these problems can be solved; others could at least be mitigated if non-forcible unilateral responses to cyber incidents of unclear origin that affect other State's interest could be better coordinated and ultimately institutionalised on the basis of an international treaty. Certainly, in the long run a cogent path would be a much stronger focus on specifying States' due diligence obligations regarding threat prevention and securing the freedom and stability of cyberspace.

---

220 See on this e.g. Segal/Waxman, 2011, Why a Cybersecurity Treaty Is a Pipe Dream, Council on Foreign Relations, 27 October 2011, available at: http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325; Goldsmith, 2011, Cybersecurity Treaties: A Sceptical View, Stanford University, available at: http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf; Jurich, 2008, Cyberwar and Customary International Law: The Potential of a 'Bottom-up' Approach to an International Law of Information Operations, 9 *Chicago Journal of International Law* 275; Lin, 2012, Arms Control in Cyberspace: Challenges and Opportunities, *World Politics Review*, 6 March 2012, available at: http://www.worldpoliticsreview.com/articles/print/11683; Maurer, 2011, Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security, Harvard Kennedy School, September 2011, available at: http://belfercenter.ksg.harvard.edu/publication/21445/cyber_norm_emergence_at_the_united_nationsan_analysis_of_the_uns_activities_regarding_cybersecurity.html.

Michael N. Schmitt

Cyber Activities and the Law of Countermeasures

1. Introduction

Contemporary legal analysis of how States may respond to malicious cyber activities has generally ignored the option of countermeasures, focusing instead on responses grounded in the law of self-defence. A customary law paradigm reflected in Article 51 of the *Charter of the United Nations* (UN Charter), the right of self-defence, permits States to respond forcefully to 'armed attacks,' including cyber operations qualifying as such.[1] The self-defence centric analytical framework reflects State fears of a possible 'cyber 9/11' in which another State or a transnational terrorist group mounts a cyber operation producing devastating human, physical, or economic consequences.

Yet preoccupation with cyber armed attacks is counter-experiential. Few, if any, cyber activities have crossed the armed attack threshold.[2] By contrast, malicious cyber operations below that level are commonplace.[3] For instance, Chinese hackers have penetrated powerful financial institutions like Morgan Stanley and the United States (US) Chamber of Commerce,[4] as well as such influential media outlets as the New York Times, Wall Street Journal, and Washington Post.[5] Reportedly, the Chinese government also hires contractors to conduct cyber operations, a prominent example being the

1 Article 51 of the UN Charter. An 'armed attack' is the textual condition precedent set forth in Article 51 for the exercise of the right of self-defence. On the customary nature of the right of self-defence, see *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 176 (June 27) [hereinafter Nicaragua]; *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, ¶¶ 38, 41 (July 8); *Oil Platforms* (Iran v. U.S.), 2003 I.C.J. 161, ¶ 74 (Nov. 6). As to self-defence in the cyber context, see Tallinn Manual On the International Law Applicable to Cyber Warfare (Michael N. Schmitt gen. ed., 2013), at rr. 13-17 and accompanying commentary; Matthew Waxman, *Self-defensive Force against Cyber Attacks: Legal, Strategic, and Political Dimensions*, 89 Int'l L. Stud. 109 (2013); Michael N. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited,* 56 Vill. L. Rev. 569, 586-603 (2011); Yoram Dinstein, *Computer Network Attacks and Self-Defense, in* Computer Network Attack and International Law 99 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

2 For instance, disagreement even exists as to whether the 2010 Stuxnet operation against the Iranian nuclear program, which damaged over 1000 centrifuges, qualified as an armed attack. *See, e.g.,* Tallinn Manual, *supra* note 1, at 58. Even if the operation rose to that level, the question remains as to whether Israel and the United States (US) enjoyed the right of anticipatory individual and collective self-defence, assuming for the sake of analysis that they were the authors of the operation.

3 For an excellent survey of the sources and techniques used to conduct such attacks, see Kenneth Geers, World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks (FireEye Labs, Sept. 24, 2013).

4 Siobhan Gorman, *China Hackers Hit U.S. Chamber*, Wall St. J., Dec. 21, 2011, at A1; Michael Gross, *Enter the Cyber-dragon*, Vanity Fair, Sept. 2011, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.

5 Nicole Perlroth, *Washington Post Joins List of News Media Hacked by the Chinese*, N.Y. Times, Feb. 1 2013, http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html; Nicole Perlroth, *Wall Street Journal Announces that it, Too, Was Hacked by the Chinese*,

'Comment Crew,' which has targeted US defence industries.[6] North Korea appears to have developed a large cyber warfare department,[7] India and Pakistan have engaged in non-destructive cyber exchanges,[8] and the Syrian Electronic Army has conducted disruptive operations against media and human rights groups it styles as anti-Assad, like Al-Jazeera, the BBC, National Public Radio, Human Rights Watch, and Anonymous.[9] And, of course, US Cyber Command possesses unparalleled capabilities to conduct operations below the armed attack threshold.

This chapter examines how and when States may employ countermeasures in response to malicious cyber operations that do not qualify as armed attacks.[10] The analysis also applies fully to the use of cyber countermeasures against non-cyber activities.[11] After discussing the nature of countermeasures, the chapter sets out the conditions precedent to taking them. It then dissects the requirements and restrictions imposed on countermeasures as they apply in the cyber context. The article concludes that countermeasures can prove an effective response option for States facing harmful cyber operations, but that due to various limitations on their use, they are no panacea. Highlighting their availability will nevertheless hopefully dampen the destabilising incentive States have to characterise cyber operations as armed attacks, if only to afford themselves a legal basis on which to ground effective responses.[12]

N.Y. Times, Jan. 31, 2013, http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html.

6 David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit is Seen as Tied to Hacking Against U.S.*, N.Y. Times, Feb. 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all; Michael Riley and Dune Lawrence, *Hackers Linked to China's Army Seen from EU to DC*, Bloomberg, July 26, 2012, http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html. A 2012 US Department of Defense report to Congress summarized the situation by asserting that 'computer systems around the world, including those owned by the U.S. government, continue [...] to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military.' Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 36 (2013), http://www.defense.gov/pubs/2013_china_report_final.pdf.

7 Max Fisher, *South Korea Under Cyber Attack: Is North Korea Secretly Awesome at Hacking?,* Wash. Post, March 20, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/20/south-korea-under-cyber-attack-is-north-korea-secretly-awesome-at-hacking/.

8 *India and Pakistan in Cyber War*, Al-Jazeera, Dec. 4, 2010, http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html.

9 Max Fisher & Jared Keller, *Syria's Digital Counter-Revolutionaries*, The Atlantic, Aug. 31, 2011, http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/; Hayley Tsukayama & Paul Farhi, *Syrian hackers claim responsibility for disrupting Twitter, New York Times Web site,* Wash. Post, Aug. 27, 2013, http://articles.washingtonpost.com/2013-08-27/lifestyle/41497149_1_syrian-electronic-army-amazon-web-services-web-site.

10 This chapter does not address the issue of where the armed attack threshold lies. On that subject, see Tallinn Manual, *supra* note 1, r. 13 and accompanying commentary.

11 Attention is slowly beginning to focus on this issue in the context of cyber operations. See, e.g., Jan E. Messerschmidt, Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm, 52 Colum. J. Transnat'l L. __ (forthcoming 2013).

12 This chapter does not address the issue of the responsibility of international organizations. On that matter, see International Law Commission, Responsibility of International Organizations, UN Doc. A/CN.4/L.778

Before proceeding, a cautionary note on terminology may prove helpful. The generic term 'cyber operation' is employed in lieu of the commonly used term 'cyber attack' to avoid confusion between cyber activities that may or may not qualify as an armed attack and those that do reach that level. 'Operations' refers to cyber activities which require affirmative action by an actor, as distinct from those which are purely passive (as with a firewall). Finally, the term operations should not be construed as necessarily denoting military character.

2. Countermeasures Generally

2.1 Countermeasures Defined

States bear 'responsibility' for their internationally wrongful acts pursuant to the law of State responsibility.[13] The International Court of Justice (ICJ) has confirmed this principle on many occasions.[14] It is the foundation upon which the authoritative, albeit non-binding, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (Articles on State Responsibility) have been constructed.[15] It is undeniable that the law of State responsibility extends to cyber activities.[16]

A remedial measure situated in the law of State responsibility, countermeasures are State actions or omissions directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel

(May 30, 2011).

13 International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Article 1, UN GA Res. 56/83 annex, UN Doc. A/RES/56/83 (Dec. 12, 2001) [hereinafter Articles on State Responsibility].

14 *See, e.g.*, *The Corfu Channel Case* (U.K. v. Alb.) [hereinafter Corfu Channel], 1949 I.C.J. 4, 23 (9 April); Nicaragua, *supra* note 1, ¶¶ 283, 292; *Case Concerning the Gabcikovo-Nagymaros Project* (Hung./Slovk.), 1997 I.C.J. 7, ¶ 47 (Sept. 25) [hereinafter Gabcikovo-Nagymaros Project]. The Permanent Court of International Justice enunciated the same principle earlier. *See, e.g.*, *Phosphates in Morocco* (It. v. Fr.), Preliminary Objections, 1938 P.C.I.J. (ser. A/B), No. 74, at 10, 28 (June 14); *Case of the S.S. 'Wimbledon'* (U.K., Fr., It. & Jap.), 1923 P.C.I.J (ser. A) No. 1, at 15, 30 (Aug. 17); *Factory at Chorzow* (Ger. v. Pol), 1927 P.C.I.J. (ser. A) No. 9, at 3, 29–30 (July 26).

15 The Articles on State Responsibility are not a treaty and therefore are non-binding. However, they are authoritative in the sense that the International Law Commission developed them during a process that took over half a century under the leadership of five special rapporteurs. Once completed, the UN General Assembly commended the Articles to governments. UN Doc. A/RES/56/83 (Jan. 28, 2001), ¶ 3. Today, they are generally, albeit not entirely, characterized as reflecting customary international law. By 2012, the Articles and the accompanying commentary had been cited 154 times by international courts, tribunals, and other bodies. United Nations Materials on the Responsibility of States for Internationally Wrongful Acts, UN Doc. ST/LEG/SER B/25 (2012). Prior to adoption of the Articles by the ILC, the US stated '[w]hile we welcome the recognition that countermeasures play an important role in the regime of state responsibility, we believe that the draft articles contain unsupported restrictions on their use.' *United States: Comments on the Draft Articles on State Responsibility,* 37 I.L.M. 468 (1998). It did not expound on its objections. For an analysis of the congruency of the Articles' approach to countermeasures with the extant law at the time of their adoption, see David J. Bederman, *Counterintuiting Countermeasures* 96 Am. J. Int'l L. 817 (2002).

16 Tallinn Manual, *supra* note 1, r. 6. On sovereignty, see *id.*, r. 1 and accompanying commentary.

or convince the latter to desist in its own internationally wrongful acts or omissions. They constitute a means of self-help in an international system generally devoid of compulsory dispute resolution methods. In that countermeasures contemplate actions that would otherwise be unlawful, international law places strict restriction on their use. These restrictions address their purpose, relationship with other legal rights and duties, means and scope of execution, originators, and targets. Both the ICJ and arbitral tribunals have recognized countermeasures.[17]

2.2 Countermeasures Distinguished

In the first half of the last century, countermeasures were labelled 'peacetime reprisals,' although that term is no longer used in deference to the neologism 'countermeasures.'[18] The historical notion of reprisals was broader than that of countermeasures in that it included both non-forceful and forceful actions.[19] Today, forceful reprisals have been subsumed into the UN Charter's use of force paradigm, which allows States to resort to force in response to armed attacks.[20] Care must likewise be taken to avoid confusing countermeasures with 'belligerent reprisals.' As will be discussed, belligerent reprisals comprise actions taken during an armed conflict that would violate international humanitarian law but for the enemy's prior unlawful conduct.[21]

The fact that countermeasures involve acts that would otherwise be unlawful distinguishes them from retortion. Retortion refers to the taking of measures that are lawful, but 'unfriendly.'[22] A State may, for instance, block certain cyber transmissions emanating from another State because the former enjoys sovereignty over cyber infrastructure on its territory.[23] The action would be lawful even if it were detrimental to the interests of the latter so long as it violated no treaty obligation or applicable customary law norm.

---

17 Gabcikovo-Nagymaros Project, supra note 14, ¶¶ 82–83 (Sept. 25); Nicaragua, supra note 1, ¶ 249. See also *Responsabilité de l'Allemagne à raison des dommages causés dans les colonies portugaises du sud de l'Afrique* ('Naulilaa') (Port. V. Ger.), II R.I.A.A. 1011, 1025–26 (1928) [hereinafter Naulilaa]; *Responsabilité de l'Allemagne en raison des actes commis postérieurement au 31 juillet 1914 et avant que le Portugal ne participât à la guerre* ('Cysne'), (Port. V. Ger.), II R.I.A.A. 1035, 1052 (1930); *Air Services Agreement of 27 March 1946* (U.S. v. Fra.), XVIII R.I.A.A. 416, 443–46 (1979) [hereinafter Air Services].

18 *See generally*, Matthias Ruffert, *Reprisals*, Max Planck Encyclopedia of Public International Law, http://opil.ouplaw.com/home/EPIL.

19 *See, e.g.*, Pearce Higgins, Hall's International Law 433-34 (8th ed. 1924); T.J. Lawrence, The Principles of International Law 311–15 (7th ed. 1910).

20 Primarily, Articles 2(4), 39, 42, 51 of the UN Charter. For a discussion of this paradigm and its customary nature, see the contributions on these articles in The Charter of the United Nations A Commentary 200, 211–13 (Bruno Simma, et al., eds., 3d ed. 2012).

21 On belligerent reprisals, see Frits Kalshoven, Belligerent Reprisals (1971).

22 Thomas Giegerich, *Retorsion*, Max Planck Encyclopedia of International Law, http://opil.ouplaw.com/home/EPIL.

23 Tallinn Manual, *supra* note 1, r. 2.

Similarly, voluntary or compulsory sanctions imposed by the Security Council pursuant to Chapter VII of the UN Charter are not countermeasures, because the Council's imprimatur renders them lawful. For example, Article 41 of the UN Charter describes interruption of communications as a non-forceful measure that may, with Security Council approval, be taken to address a threat to the peace, breach of the peace, or act of aggression.[24] Thus, a Security Council Resolution authorising interference with a State's cyber capabilities by damaging cyber infrastructure located in that State would render the activity lawful, and hence not a countermeasure, even if doing so would otherwise have infringed on the target State's sovereignty.[25] In the same vein, although countermeasures often consist of acts that violate a treaty, simply terminating a treaty relationship pursuant to the treaty's terms does not qualify as a countermeasure.[26]

Countermeasures must also be distinguished from actions taken based on a plea of necessity. Faced with a situation threatening 'grave and imminent peril' to an 'essential interest' (whether in the cyber realm or not), a State may take measures, including actions that would otherwise be internationally wrongful, to safeguard those interests.[27] The measures may be either cyber or non-cyber, or a combination thereof. Actions based on the plea of necessity differ from countermeasures in three ways. First, there need be no underlying internationally wrongful act to justify them. Second, the originator of the precipitating act need not be a State, or indeed, even be identified, a particularly relevant consideration with respect to cyber operations. Third, action based on necessity is only available when the situation is dire; mere international wrongfulness does not suffice to trigger this response option, as it does with respect to countermeasures.[28] In the cyber context, the plea of necessity is most likely relevant when cyber operations threaten the operation of critical cyber infrastructure.

3. Conditions Precedent to Countermeasures

Countermeasures may only be taken in response to an internationally wrongful act. Such acts have two components: first, breach of an international obligation, and second attribution of the wrongful act to the State in question.[29] In the law of State responsibility,

24 Article 41 of the UN Charter.

25 In practical terms, such a measure is feasible only with respect to a country with a limited number of cables connecting its 'domestic internet' with the external net. However, it would be nearly impossible to conduct against a large nation like the US, especially in light of the added factor of satellite connectivity.

26 Article 42 of the *Vienna Convention on the Law of Treaties*, May 23, 1969, 1155 U.N.T.S. 331.

27 Articles on State Responsibility, *supra* note 13, Article 25. *See also* Gabcikovo-Nagymaros Project, *supra* note 14, ¶¶ 51, 55; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. 136, ¶ 140 (9 July).

28 The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries, 178–86 (James Crawford Special Rapporteur 2002) [hereinafter Articles on State Responsibility Commentary]. The Cambridge University Press publication reprints the official International Law Commission's Articles and accompanying commentary. *See also* Tallinn Manual, *supra* note 1, at 39–40.

29 Articles on State Responsibility, *supra* note 13, Article 2.

the State breaching the obligation is known as the 'responsible State,' whereas the State to which the obligation is owed is styled the 'injured State.'

So long as these two conditions are satisfied and there is full compliance with the requirements and limitations set out below, countermeasures, whether cyber or non-cyber in character, are allowable. For example, in 1998 the US military launched an operation against a hacktivist group, the Electronic Disturbance Theater, which had targeted the Pentagon with a denial of service (DoS) attack.[30] Qualification of the 'hack back' as a lawful countermeasure would depend on identifying a violation of international law by the hacker group and determining if and how the group's activities were connected to another State.

3.1 Breach of an International Obligation

An internationally wrongful act breaches the responsible State's international obligations to the injured State.[31] The concept of breach in this context does not extend to violations of domestic legal regimes.[32] When a State has 'injured' another State, group of States, or the international community, the injured State(s) may invoke the international responsibility of the responsible State and demand cessation and (or) reparations.[33]

The breach in question may consist of a violation of either a State's treaty obligations or customary international law. For instance, a State that conducts cyber operations directed against a coastal nation from a ship located in the latter's territorial sea is in breach of the innocent passage regime set out in both the *United Nations Convention*

30 Winn Schwartau, *Striking Back*, Network World Fusion (Jan. 11, 1999), http://www.networkworld.com/news/0111vigilante.html.

31 Articles on State Responsibility, *supra* note 13, Article 2; Articles on State Responsibility Commentary, *supra* note 28, at 81. *See* also *Phosphates in Morocco*, *supra* note 14, at 28 ('This act being attributable to the State and described as contrary to the treaty right of another State, international responsibility would be established immediately as between the two States'); *United States Diplomatic and Consular Staff in Tehran* (U.S. v. Iran), 1980 I.C.J. 3, ¶ 56 (May 24) [hereinafter Teheran Hostages]. Note that the requirement that the breach violate international law is stringent. As stated by the ICJ, 'it is entirely possible for a particular act [...] not to be in violation of international law without necessarily constituting the exercise of a right conferred by it.' *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion, 2010 I.C.J. 403, ¶ 56 (22 July). An example of such a situation is espionage, which, albeit not a violation, is equally not a right enjoyed by States. Of course, the conduct underlying an act of cyber espionage, such as an intrusive act causing damage to a cyber system, could violate international law. Tallinn Manual, *supra* note 1, at 193–94.

32 Articles on State Responsibility, *supra* note 13, Article 3.

33 *Id.*, Article 30, 31, 34–37, 42, 48(1). Reparations may take the form of restitution, compensation, and satisfaction. *Id.*, Article 34. Restitution involves the reestablishment of the situation that existed prior to the internationally wrongful act. *Id.,* Article 35. Compensation involves financial payment for damage incurred by the internationally wrongful act to the extent that the damage is not made good by restitution. *Id.*, Article 36 (1). Satisfaction consists of 'an acknowledgment of the breach, an expression of regret, a formal apology or other appropriate modality.' *Id.*, Article 37(2).

on the Law of the Sea[34] and customary international law.[35] Similarly, a State's aircraft non-consensually engaging in cyber operations above the territorial sea of another State is violating treaty and customary law.[36]

Especially prominent among the relevant customary norms is the principle of sovereignty, which, as noted in the *Island of Palmas* arbitration, 'signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[37] In the cyber context, sovereignty grants a State the right (and in some cases the obligation) to regulate and control cyber activities and infrastructure on its territory.[38] Territorial sovereignty also protects cyber infrastructure located on a State's territory, regardless of its governmental character, or lack thereof. Consequently, hostile cyber operations against cyber infrastructure on another State's territory amount to, *inter alia,* a violation of that State's sovereignty if they cause physical damage or injury.[39] Of course, interference with cyber infrastructure aboard a sovereign platform is also a violation of the respective State's sovereignty no matter where the platform is located.[40]

Some international law experts take the position that sovereignty can at times be violated even when no damage results, as in the case of emplacement of malware designed to monitor a system's activities.[41] This approach is the more defensible one when considered in light of the principle of sovereignty's object and purpose. Sovereignty is meant to afford States the right to conduct, or allow, activities on their territory free from interference by other States. While monitoring activities in another State may merely constitute espionage, which is not prohibited, emplacement of malware into a system, destruction of data, and hacking into a network to identify vulnerabilities would seem to pierce the veil of sovereignty. Recent reports of Iranian hackers penetrating US energy companies to acquire information on how to disrupt operations or destroy facilities

34 See, esp., Article 17 & 19 of the *United Nations Convention on the Law of the Sea*, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter Law of the Sea Convention].

35 The US is not a party to the Law of the Sea Convention, but recognizes the right of innocent passage, and the limitations thereon, as customary in nature. *See* U.S. Navy/U.S. Marine Corps/U.S. Coast Guard, The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, ¶ 2.5.2.1 (2007).

36 International Civil Aviation Organization, *Convention on International Civil Aviation*, Article 1, Dec. 7, 1944, 15 U.N.T.S. 295; Law of the Sea Convention, *supra* note 34, Article 2(2); NWP 1-14M, *supra* note 35, ¶ 1.9; Harvard Program on Humanitarian Policy and Conflict Research, Manual on International Law Applicable to Air and Missile Warfare, r. 1(a) and accompanying commentary (2013).

37 *Island of Palmas* (Neth. v. US), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

38 Tallinn Manual, *supra* note 1, r. 1. Cyber infrastructure refers to '[t]he communications, storage, and computing resources upon which information systems operate. The Internet is an example of a global information infrastructure.' *Id.* at 258.

39 *Id.* at 16. This assumes there is no legal justification for the operations, such as self-defence or the taking of countermeasures (see discussion *infra*).

40 *Id.*, r. 4. The cyber infrastructure concerned must serve exclusively governmental purposes. *Id.* at 24.

41 *Id.* at 16.

illustrate the weakness of requiring damage as an essential element of a sovereignty violation.[42] Similarly, assuming attribution to Iran, the Shamoon virus attacks that erased thousands of Saudi Aramco's hard drives without physically damaging them in 2012 should likewise be styled as a violation of Saudi Arabia's sovereignty.[43]

Cyber operations into another State violate the principle of non-intervention, and accordingly qualify as internationally wrongful acts, when intended to coerce (as distinct from merely influencing) the targeted State's government in matters reserved to that State. Damage need not result.[44] As explained by the ICJ in the *Nicaragua* case, 'the principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States.'[45] In that case, the Court held that supplying funds to guerrilla forces in another country, although not a use of force in violation of Article 2(4) of the UN Charter,[46] amounted to an unlawful intervention.[47] By this finding, funding a non-State group's cyber operations that rise to the level of a use of force would likewise constitute an intervention. Other examples that violate the principle of intervention include manipulation of public opinion polls on the eve of an election or bringing down the online services of a political party.[48]

International law also imposes duties on States, the omission of which can qualify as a breach in the law of State responsibility. Conspicuous among these is the requirement that States maintain control over activities on their territory, an obligation the ICJ acknowledged in its first case, *Corfu Channel*. There, the Court held that a State may not 'allow knowingly its territory to be used for acts contrary to the rights of other States.'[49]

Based on this duty, the *Tallinn Manual*, a non-binding study produced by an 'International Group of Experts' in 2013, asserts that '[a] State shall not knowingly allow the cyber

---

42 Siobhan Gorman & Danny Yadron, *Iran Hacks Energy Firms, U.S. Says*, Wall St. J., May 23, 2013, http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968.

43 Christopher Bronk & Eneken Tikk-Rigas, *The Cyber Attack on Saudi Aramco*, Survival, April–May 2013, at 81.

44 Tallinn Manual, *supra* note 1, at 43–45.

45 Nicaragua, *supra* note 1, ¶ 205. *See also* Corfu Channel, *supra* note 14, at 35. The prohibition derives from the principle of the sovereign equality of States as codified in Article 2(1) of the UN Charter. It is specifically acknowledged in the *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UN GA Res. 2625, Annex, 25 UN GAOR, Supp. (No. 28), UN Doc. A/5217 at 121 (1970). *See also* Article 4(g) of the *Constitutive Act of the African Union*, July 11, 2000, OAU Doc. CAB/LEG/23.15 (entered into force May 26, 2001); Article 19 of the *Charter of the Organization of American States*, Apr. 30, 1948, 119 U.N.T.S. 3. On intervention, see Philip Kunig, *Prohibition of Intervention*, Max Planck Encyclopedia of Public International Law (2008), http://opil.ouplaw.com/home/EPIL.

46 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.' As to the norm's customary international law nature, see Nicaragua, *supra* note 1, ¶¶ 188–90.

47 Nicaragua, *supra* note 1, ¶ 228.

48 Tallinn Manual, *supra* note 1, at 45.

49 Corfu Channel, *supra* note 14, at 22–23. *See also* Tehran Hostages, *supra* note 31, at 67–68; *The Trail Smelter Arbitration Case* (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (Apr. 16, 1938).

infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.'[50] States are required to use their 'best efforts' to comply with the obligation.[51] In that harmful cyber operations are often launched by non-State actors like 'hacktivists,' and in light of the imminent advent of 'cyber terrorism,' a State's obligation to control cyber activities taking place on its territory looms especially large.[52]

Various circumstances preclude the wrongfulness of a State's acts or omissions, all of which apply fully in the cyber context. A State's consent to a cyber operation by another State bars it from subsequently claiming that the act breached an obligation it was owed.[53] For example, one State may allow another State to temporarily take control of certain facets of its cyber infrastructure in order to allow the latter to identify and respond to malicious activities occurring therein. Should this occur, the former cannot claim injury, at least so long as the cyber activities in question were within the scope of the consent. Additionally, the wrongfulness of a cyber use of force is precluded if it qualifies as legitimate self- or collective defence,[54] or has been authorized by the UN Security Council.[55] Force majeure, distress, and necessity likewise preclude the wrongfulness of an act or omission, as does a need to comply with a peremptory norm of international law.[56]

Finally, qualification of an act as a countermeasure, the subject of this article, excludes the wrongfulness of an act.[57] As acknowledged in the *Tallinn Manual*, '[a] State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.'[58] In other words, a

---

50 Tallinn Manual, *supra* note 1, r. 5. The obligation applies when State organs or entities under governmental control can take the remedial action. The International Group of Experts associated with the Tallinn Manual project also agreed 'if a remedial action could only be performed by a private entity, such as a private Internet service provider, the State would be obliged to use all means at its disposal to require that entity to take the action necessary to terminate the activity.' Tallinn Manual, *supra* note 1, at 28.

51 Articles on State Responsibility Commentary, *supra* note 28, at 140.

52 The Tallinn Manual's International Group of Experts could not agree on whether the obligation was borne by State through whose territory the offending cyber operation passed. Tallinn Manual, *supra* note 1, at 28.

53 Articles on State Responsibility, *supra* note 13, Article 20.

54 *Id*., Article 21; Article 51 of the UN Charter.

55 Article 42 of the UN Charter.

56 Articles on State Responsibility, *supra* note 13, Articles 23–26. To illustrate, assume one State is legally obligated to maintain particular cyber communications with another State. An example of force majeure would be interruption of cyber communications due to a natural disaster. Distress would be exemplified by interrupting them due to the risk of malware infection from a third State. Shutting off cyber communications in order to ensure the infrastructure is not used to incite genocide would represent the third factor precluding wrongfulness.

57 Articles on State Responsibility, *supra* note 13, Article 22. In international law, acts are generally lawful unless expressly prohibited. *The Case of the S.S. 'Lotus'* (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 3, 18 (Sept. 7). Thus, a countermeasure does not render an action permissible; rather, qualification as such keeps it from being unlawful.

58 Tallinn Manual, *supra* note 1, r. 9, which is based on Articles 22 and 49–53 of the Articles on State Responsibility, *supra* note 13.

countermeasure is not an internationally wrongful act, and countermeasures may not be taken in response to legitimate countermeasures.

3.2 Attribution to a State

Countermeasures are only available when the precipitating breach is attributable to a State pursuant to the law of State responsibility.[59] Therefore, to understand the permissible targets of countermeasures, it is necessary to consider the scope of attribution under that body of law.

Attribution is appropriate in a number of circumstances.[60] The clearest case is when State organs, such as the military or intelligence agencies, engage in the wrongful acts.[61] For instance, all cyber activities of US Cyber Command or the National Security Agency are fully attributable to the US and engage its responsibility under international law.

Confirming that a governmental organ originated a cyber operation can prove challenging even when launched from government cyber infrastructure. In particular, such infrastructure is susceptible to exploitation by non-State actors. Moreover, the groups or individuals involved may intentionally try to create the impression that a particular State was behind the operation ('spoofing'). The need to respond promptly to some cyber operations can complicate the attribution dilemma.

Cognizant of this reality, the *Tallinn Manual* concludes that although '[t]he mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indication that the State in question is associated with the operation.'[62] Reliable intelligence that a non-State group will attempt to spoof the origin of hostile cyber operations would, for example, auger against any such conclusion. So too would the existence of friendly relations between the injured State and the purported responsible State. When feasible, a State that is believed to be responsible for a cyber operation because the precipitating cyber operation originated from its cyber infrastructure should be afforded an opportunity to rebut the assumption. Understandably, each situation must be considered in context.

The fact that a harmful cyber operation has been mounted using private cyber infrastructure, or has simply been routed through governmental or non-governmental cyber infrastructure in a State's territory, does not suffice to indicate association.[63]

---

59 Articles on State Responsibility, *supra* note 13, Article 2(a).

60 Tallinn Manual, *supra* note 1, r. 6.

61 Articles on State Responsibility, *supra* note 13, Article 4(1).

62 Tallinn Manual, *supra* note 1, r. 7.

63 See the exclusion of other than governmental cyber infrastructure in Tallinn Manual, *supra* note 1, r. 7, and *id.*, r. 8 and accompanying commentary. In Corfu Channel, *supra* note 14, at 18, the ICJ stated that 'it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State

This is a particularly important limitation given the possibility of creating botnets using zombie computers in multiple countries to mount distributed DoS attacks. As an illustration, in 2013 a North Korean cyber operation shut down thousands of South Korean media and banking computers and servers. The operation employed more than 1,000 Internet Protocol (IP) addresses in 40 countries.[64] Obviously, most, if not all, of the countries involved were completely unassociated with the operation.

As discussed, the failure of a State to take feasible measures to terminate harmful cyber operations originating in its territory also constitutes an internationally wrongful omission by that State. Injured States taking countermeasures based on such a breach must be cautious. In particular, the proportionality of the countermeasure (a requirement that is examined below) will be determined with respect to the responsible State's failure to properly police its territory. It will not be judged solely against the severity and consequences of the offending cyber operations that the responsible State had a duty to terminate. In other words, the harmful cyber operation is not 'imputed' to the State from which it was launched. Rather, the countermeasure must be designed to compel the responsible State to police the cyber infrastructure and activities on its territory.

Acts committed by persons or entities that do not qualify as State organs, but which are empowered by domestic law to exercise elements of governmental authority, are equally attributable to the State, albeit only with respect to the exercise of said authority.[65] The persons or entities are essentially equated to State organs for the purposes of the law of State responsibility. Examples include a private sector Computer Emergency Response Team (CERT) authorised to protect State activities and a private company that has been contracted to conduct offensive cyber operations for the military or to gather intelligence by cyber means on behalf of the State's intelligence agencies. The key is that the acts in question must be of a governmental character and performed based on legal authorisation, such as legislation or contract, from the State.

In the case of activities by either State organs or entities empowered to exercise elements of governmental authority, the State bears responsibility even when the conduct in question is *ultra vires,* that is, exceeds the authority granted by the State or contravenes the State's instructions.[66] To take a simple example, if a member of a government's

---

necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known the authors.'

64 Lance Whitney, *North Korea Behind March Cyber Attack, says South Korea*, C/NET, Apr. 10, 2013, http://news.cnet.com/8301-1009_3-57578829-83/north-korea-behind-march-cyberattack-says-south-korea/.

65 Articles on State Responsibility, *supra* note 13, Article 5. Note that pursuant to Article 6, if the organ of a State is placed at the disposal of another State to exercise elements of governmental authority, the conduct of that organ is attributable to the latter. In such a case, only the State which the organ was placed at the disposal of bears responsibility for the actions. Articles on State Responsibility Commentary, *supra* note 28, at 145.

66 Articles on State Responsibility, *supra* note 13, Article 7. It is unsettled whether the State where the cyber infrastructure is located has an obligation to take measures to prevent prospective harmful cyber operations. See discussion in Tallinn Manual, *supra* note 1, at 27.

CERT conducts unlawful activities in defiance of orders to the contrary, the member's State incurs responsibility for any breach of obligations owed to other States.

The actions of one State can occasionally result in the responsibility of another, thereby opening the door to countermeasures directed against both (assuming the act or omission violates an obligation owed by each to the injured State). This possibility arises in three circumstances. First, a State aiding the commission of an internationally wrongful act by another will bear responsibility if it does so knowing the circumstances surrounding the unlawful act and whether the act would have been wrongful if committed by the State providing the assistance.[67] A case in point would be allowing another State to use the assisting State's cyber infrastructure to mount the offending operation. Similarly, a State will be responsible for a cyber operation conducted by another State if it finances the operation. The requirement that the State know of the circumstances of the internationally wrongful act is critical in this regard. For instance, if a State finances the acquisition of cyber capabilities by another without knowing that those capabilities will be used to conduct harmful acts, it would bear no responsibility for them.

Care must be taken in the application of this rule. When a State's assistance is an essential aspect of an operation, as in allowing its cyber infrastructure to be used in order to conduct the operation, the State will be responsible for the injury suffered and subject to countermeasures on that basis. Yet, if the assistance is not an integral component of the wrongful act, the assisting State will be responsible for the support alone, and subject only to countermeasures that are proportionate to said assistance. This might be the case if the said State merely provides some of the operations financing.[68]

The second basis for a State's responsibility for another State's wrongful cyber operation exists when the former directs and controls the latter's commission of the operation.[69] The State mounting the operation essentially serves as a surrogate; therefore, the State exercising direction and control is fully responsible for its surrogate's actions and subject to countermeasures that would be an appropriate response to the cyber operation itself. These situations are rare, as States, while perhaps subject to other States' influences, are seldom in their control. Occupation is the most relevant contemporary illustration.

Coercion is the third basis for rendering a State responsible for another State's wrongful acts.[70] The level of coercive effect must be very high; '[n]othing less than conduct which forces the will of the coerced State will suffice, giving it no effective choice but to

67 Articles on State Responsibility, *supra* note 13, Article 16. With respect to the wrongfulness requirement *vis-à-vis* the assisting State, note that a State is not bound by the obligations of another State with regard to third States. *See, e.g.*, Articles 34–35 of the *Vienna Convention on the Law of Treaties*, May 23, 1969, 1155 U.N.T.S. 331.

68 Articles on State Responsibility Commentary, *supra* note 28, at 151.

69 Articles on State Responsibility, *supra* note 13, Article 17.

70 *Id.*, Article 18.

comply with the wishes of the coercing State.'[71] As an example, a State might threaten serious cyber attacks against a coerced State if the latter does not engage in a particular cyber operations, such as altering critical data of a third State stored on servers located in the coerced State.

Attribution of the acts of individuals or entities that are neither State organs, nor empowered to exercise governmental functions, is of particular importance in the cyber context. Generally, the acts of private actors are not attributable to States. However, Article 8 of the Articles on State Responsibility provides '[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.'[72] Note that there is no requirement that the activities be inherently governmental in character.

The 'on the instructions' situation would present itself when a group of private individuals that has been recruited or instigated by a State operates as its auxiliary without being specifically commissioned to do so pursuant to the domestic legal regime, as with a group of volunteers who conduct cyber operations on behalf of a State. The group, although not forming a part of any organisation in the State structure, might, for example, perform particular functions within the State's cyber operations system, like identifying vulnerabilities in cyber infrastructure that are later exploited by the State's cyber units. The group is effectively part of the State's cyber forces. In such a case, States injured by the group's activities could resort to countermeasures against the 'sponsoring' State.

Article 8 situations can also involve groups or individuals that act 'under the direction or control' of the State for particular activities.[73] As an example, one State may direct the actions of a group of hacktivists sharing its ethnicity or religion that is based in another State. If that group engages in harmful cyber operations against the latter at the behest of the former, the former will be responsible for those activities. Since the relationship with the State is more extenuated than in the previous 'auxiliary' case, their conduct 'will be attributable to the State only if it directed or controlled the specific

71 Articles on State Responsibility Commentary, *supra* note 28, at 156.

72 Articles on State Responsibility, *supra* note 13, Article 8. This issue was addressed in the most authoritative US statement on the law of cyber operations to date, a speech by the (then) US State Department Legal Adviser. Harold H. Koh, *International Law in Cyberspace*, Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland (Sept. 18, 2012), *reprinted in* 54 Harv. Int'l L.J. Online 1, 6–7 (2012). The Koh address and the *Tallinn Manual* are compared in Michael N. Schmitt, *The Koh Speech and the Tallinn Manual Juxtaposed*, 54 Harv. Int'l L.J. Online 13 (2012).

73 Articles on State Responsibility, *supra* note 13, Article 8.

operation and the conduct complained of was an integral part of that operation.'[74] Recent reports of 'cyber mercenaries' illustrate these situations.[75]

Incidental or peripheral association with a State's cyber operations does not warrant attribution. The hacktivist operations against Estonia and Georgia in 2007 and 2008 respectively were not, at least on the available evidence, sufficiently under Russia's control to justify attribution, and therefore countermeasures, by those countries against Russia.[76] Similarly, in April 2013, the Syrian Electronic Army tweeted from the Associated Press's Twitter account that President Obama had been wounded during an attack on the White House. The Dow Jones Industrial Average dropped 143 points, resulting in a USD136 billion loss within a few minutes.[77] Yet, in the absence of direction and control by Syria, countermeasures were unavailable as a response option (even if assuming a breach of an obligation).

In light of the growing ability of individuals and private groups to mount harmful cyber operations against States, these situations are likely to become increasingly common. The complexity of establishing the connection to the State is also an obstacle, a reality well-demonstrated by Mandiant's analysis of the actions of the cyber espionage group APT1.[78] Of course, as discussed, States have a duty to control cyber operations being conducted from their territory and failure to do so may provide a separate ground for countermeasures.

The possibility of attributing acts based on a State's direction and control of non-State actors begs the question of the requisite degree of direction and control. In the *Nicaragua* case, the ICJ posed the question of whether the US was responsible for the acts of the *contra* insurgents against the government of Nicaragua. The Court held that '[f]or this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that the State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.'[79]

This standard should not be confused, as it often is, with the 'overall control' test set forth by the International Criminal Tribunal for the Former Yugoslavia's Appeals

74 Articles on State Responsibility Commentary, *supra* note 28, at 110.

75 Zachary Fryer-Biggs, New Cyber 'Mercenaries' Prefer Quick Strikes, Researchers Say, Defense News, Sept. 27, 2013, http://www.defensenews.com/article/20130927/DEFREG02/309270009/New-Cyber-Mercenaries-Prefer-Quick-Strikes-Researchers-Say?odyssey=nav%7Chead; Jeb Boone, Mercenary Hacker Group 'Hidden Lynx' Emerges as World's Most Potent Cyber Threat, GlobalPost, Sept. 18, 2013.

76 On the incidents, see Eneken Tikk, Kadri Kaska & Liis Vihul, International Cyber Incidents: Legal Considerations (2010).

77 Steven Stalinsky, China Isn't The Only Source Of Cyberattacks, Wall St. J., May 22, 2013, at 17.

78 Mandiant, APT1: Exposing One of China's Cyber Espionage Units (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

79 Nicaragua, *supra* note 1, ¶ 115.

Chamber in the *Tadic* case.[80] There, the Tribunal dealt with the issue of the relationship between States and non-State actors, but only with respect to whether the armed conflict in Bosnia-Herzegovina was international in character, based on the link between the Federal Republic of Yugoslavia and the Bosnian Serb forces. In its *Genocide* judgment, the ICJ correctly distinguished the two standards, affirming that for the purpose of attribution under the law of State responsibility, the effective control test was the proper one.[81] Therefore, a State has to be in effective control and direction of a group conducting cyber operations before countermeasures may be used; it must be acting on the State's behalf. Providing financial or other support for the operations falls short. Indeed, as the Court noted in *Nicaragua*, 'even the general control [...] over a force with a high degree of dependency on it' does not constitute effective control.[82]

An interesting situation involves State-owned companies, such as an information technology (IT) firm. State ownership of a company alone is insufficient to attribute its actions to the State such that countermeasures are available against the State for the wrongful conduct of the firm.[83] However, if the company engages in cyber operations that comprise a governmental function, or if the operations in question are conducted under the State's effective control and direction, its activities are attributable to the State and countermeasures against the State are appropriate in relation to those actions.

It must be cautioned that geography is irrelevant to the issue of attribution. Non-State actors may, and likely often will, launch a cyber operation from outside territory controlled by the State to which the conduct is attributable. A paradigmatic example would involve non-State actors in one State under the direction and control of another State assimilating computers located in multiple States into a botnet, and using the botnet to target the injured State. The determinative issue is the level of direction and control, not the location of the activities.

Finally, and unlike situations involving State organs or those exercising governmental functions, attribution based on direction and control does not extend to acts exceeding the direction. In other words, acts that clearly exceed the State's instructions do not result in attribution.[84] For instance, if a State instructs a hacktivist group in another country not to target critical cyber infrastructure, and the group nevertheless does so, the group's actions will provide no basis for taking countermeasures against the State.

---

80 *Prosecutor v. Tadić*, Case No. IT-94-1-A, Appeals Chamber Judgment ¶¶ 117, 131–40, 145 (Intl'l Crim. Trib. for the Former Yugoslavia, July 15, 1999).

81 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosn. & Herz. v. Serb. & Montenegro.), 2007 I.C.J. 108, ¶¶ 403–05 (Feb. 26).

82 Nicaragua, *supra* note 1, ¶ 115.

83 Articles on State Responsibility Commentary, *supra* note 28, at 112.

84 *Id*. at 113.

4. Countermeasures Requirements and Restrictions

4.1 Purpose of Countermeasures

The sole permissible purpose of countermeasures is to return a situation to lawfulness.[85] Therefore, as noted in the Articles on State Responsibility, a State that is responsible for an internationally wrongful act against another State is obliged to cease an ongoing act (or rectify an omission) and to 'offer appropriate assurances and guarantees of non-repetition if circumstances so require.'[86] Moreover, if the internationally wrongful act has caused injury, the responsible State must provide reparations for that injury. The term 'injury' refers to any material or moral damage caused by the internationally wrongful act.[87] Countermeasures are not permissible for other purposes, such as retaliation or punishment.

Reflecting the purpose of inducing a return to lawful relations between the States concerned, the ICJ has opined that countermeasures must generally be reversible; they should, as far as possible, be taken in such a way as to permit the resumption or performance of the obligations involved in the countermeasure.[88] This requirement is not absolute. For instance, a countermeasure in form of a DoS can be terminated and the blocked service restored, but the activities that were interrupted may not be able to be performed later. This would not bar the countermeasure. This said, countermeasures are generally viewed as temporary measures and therefore 'must be as far as possible reversible in their effects in terms of future legal relations between the two States.'[89]

Since their sole purpose is to incentivise the resumption of lawful interactions, the risk of escalation should be taken into account when deciding whether, and how, to engage in countermeasures. Relatedly, a countermeasure that will only exacerbate the situation is mere retaliation (although it would seem that States sometimes *de facto* act in retaliation). Thus, as noted in the *Air Services* arbitration, '[c]ounter-measures [...] should be a wager on the wisdom, not on the weakness of the other Party. They should be used with a spirit of great moderation and be accompanied by a genuine effort at resolving the dispute.'[90] This cautionary note is especially relevant with regard to cyber countermeasures, because the speed with which the precipitating hostile cyber

85 Articles on State Responsibility, *supra* note 13, Article 49(1). In *Archer Daniels Midland Company v. Mexico*, Mexico's argument that a tax was lawful as a countermeasure was rejected on the basis that Mexico did not impose it in order to compel the US to comply with its obligations. Award, ICSID Case No. ARB(AF)/04/05, ¶¶ 134–51 (Nov. 21, 2007).

86 Articles on State Responsibility, *supra* note 13, Article 30.

87 *Id.*, Article 31.

88 Gabcikovo-Nagymaros Project, *supra* note 14, ¶ 87; Articles on State Responsibility, *supra* note 13, Article 49(3).

89 Articles on State Responsibility Commentary, *supra* note 28, at 283.

90 Air Services, *supra* note 17, Article 91.

operations may unfold poses a particular risk of rapid retaliatory exchange that leaves little time for the careful consideration of possible consequences.

Lastly, in that they are intended to induce a return to lawful relations, countermeasures are reactive, not prospective. As the ICJ observed in the *Gabcikovo-Nagymoros Project* case, they 'must be taken in response to a previous internationally wrongful act of another State.'[91] There is no countermeasure equivalent to anticipatory self-defence against a prospective cyber armed attack.[92] Nor may countermeasures be employed for deterrent purposes.

4.2 Situations Precluding Countermeasures

Since they are designed to impel a return to lawful relations between the States involved, countermeasures may not be taken in response to an internationally wrongful act that is complete and unlikely to be repeated.[93] Article 53 of the Articles on State Responsibility provides that, '[c]ountermeasures shall be terminated has soon as the responsible State has complied with its obligations [of cessation and reparation] in relation to the internationally wrongful act.'[94] Note that if reparations are due, the countermeasures may continue even though the wrongful act has ended. Additionally, countermeasures remain available when the internationally wrongful act is but one in a series of wrongful acts. As an example, if an injured State had been subjected to a series of DoS attacks such that it would be reasonable to conclude that further attacks will take place, the injured State may take countermeasures to induce the responsible State to desist from its pattern of conduct.

In light of their purpose, countermeasures must be suspended when the internationally wrongful act has ceased and the dispute in question is pending before a 'court or tribunal' that may issue a binding decision in the matter.[95] Given that a judicial body is handling the situation, the element of necessity is missing. The phrase 'court or tribunal', drawn from the Articles on State Responsibility, refers to 'any third-party dispute settlement procedure, whatever its designation.'[96]

91 Gabcikovo-Nagymaros Project, *supra* note 14, ¶ 83.

92 On anticipatory self-defence, see Tallinn Manual, *supra* note 1, at 63-66; Terry D. Gill & Paul A.L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 Int'l L. Stud. 438 (2013).

93 Articles on State Responsibility, *supra* note 13, Article 49(2), Article 52(3)(a). *See also* Maurice Kamto, *The Time Factor in the Application of Countermeasures*, in The Law of International Responsibility 1169 (James Crawford, Alain Pellet & Simon Olleson eds. 2010).

94 *Id.*, Article 53.

95 Articles on State Responsibility, *supra* note 13, Article 52(3).

96 Articles on State Responsibility Commentary, *supra* note 28, at 299. The term does not include cases that have been referred to political entities such as the United Nations Security Council. *Id.*

This prohibition applies only once the case is *sub judice*.[97] While it might appear that such a limitation runs counter to the goal of resuming lawful relations, it can be argued that countermeasures provide an incentive to agree to binding arbitration or referral to a judicial body.[98] Additionally, the exclusion of cases that are *sub judice* is tempered by the condition that the court or tribunal in question must enjoy the authority to order 'interim measures of protection, regardless of whether this power is expressly mentioned or implied in its statute (at least as the power to formulate recommendations to this effect).'[99] Should the judicial body lack such power, or if the exercise thereof is significantly restricted, the injured State may retain the right to initiate or maintain countermeasures.[100]

A further obstacle to countermeasures is that, as recognized by the *Naulilaa* arbitration with respect to reprisals, a request for the responsible State to remedy the internationally wrongful act must precede the measure.[101] The ICJ has confirmed that this requirement applies to countermeasures. In *Gabcikovo-Nagymaros*, the Court held that before a countermeasure may be taken, 'the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it.'[102] The Articles on State Responsibility, which require an injured State to specify the conduct that it deems unlawful and the form reparations should take, likewise reflect the requirement.[103] An injured State must afford the responsible State an opportunity to respond to its request. Moreover, the former must notify the latter of any decision to take countermeasures and offer to negotiate on the matter, although in some cases it is reasonable to provide both notifications simultaneously.[104]

These requirements are sensible in light of the fact that a countermeasure, by definition, involves a breach of what would otherwise be the injured State's international law obligation towards the responsible State. They accordingly comport with international law's preference for solutions to disputes that minimise the potential for escalatory illegality. In the case of cyber operations, the conditions are especially apt because the originator of an attack may be spoofed, or, in the case of a failure to terminate activities from a State's territory, the territorial State may be unaware of the activities.

---

97 Air Services, *supra* note 17, at ¶ 95. Additionally, the court or tribunal must exist and enjoy jurisdiction over the matter. For instance, the limitation does not apply to an *ad hoc* tribunal established by treaty, which has not yet been formed. Articles on State Responsibility Commentary, *supra* note 28, at 299.

98 *See, e.g.*, Air Services, *supra* note 17, ¶ 95.

99 *Id.*, ¶ 96.

100 *Id.*

101 Naulilaa, *supra* note 17, at 1026. *See also* generally Yuji Iwasawa & Naoki Iwatsuki, *Procedural Conditions,* in The Law of International Responsibility, *supra* note 93, at 1149. Note that the arbitration dealt with forcible reprisals, which would not quality as countermeasures. That said, the decision is viewed as the key early case in the development of this body of law.

102 Gabcikovo-Nagymaros Project, *supra* note 14, ¶ 84. *See also* Air Services, *supra* note 17, ¶¶ 85–87.

103 Articles on State Responsibility, *supra* note 13, Articles 43(2) & 52(1)(a).

104 *Id.*, Article 52(1)(b); Articles on State Responsibility Commentary, *supra* note 28, at 298.

However, the requirements are not categorical. In certain circumstances it may be necessary for an injured State to act immediately in order to preserve its rights and avoid further injury. When such circumstances arise, the injured State may launch countermeasures without notification of its intent to do so.[105] As an example, assume that very serious wrongful cyber operations are underway against the injured State's banking system. The injured State can respond with cyber countermeasures designed to block electronic access to the responsible State's bank accounts. However, notifying the responsible State of its intent to do so would afford that State an opportunity to transfer assets out of the country or to address the vulnerabilities to be exploited, thereby effectively depriving the injured State of the possibility of taking such countermeasures.

Moreover, as the *Air Services* arbitration reasonably observed, 'it is [not] possible, in the present state of international relations, to lay down a rule prohibiting the use of countermeasures during negotiations [...].'[106] There is no duty to abstain from countermeasures during negotiations that are not being conducted in good faith[107] or when the internationally wrongful acts are still underway and causing significant injury. Additionally, ongoing negotiations cannot bar countermeasures indefinitely. 'What constitutes a reasonable duration of a negotiation will in fact depend on the circumstances, including the attitude of the responsible State, the urgency of the question at stake, the likelihood that damage may be exacerbated if a speedy resolution is not achieved, etc.'[108]

An unresolved issue is whether 'amicable' means of settling a dispute (as distinct from mere negotiations) involving adverse cyber operations must be exhausted before countermeasures are pursued. It is sometimes suggested that such an obligation derives from Articles 2(3) and 33 of the UN Charter, which set forth the principle of peaceful settlement of dispute.[109] The counterargument is that countermeasures, in that they do not involve the use of force, already qualify as peaceful means of settling a dispute. By this line of reasoning, amicable settlement, that is, settlement by means that would otherwise be lawful, is not required.[110] The most judicious approach would be one that assesses whether 'amicable' measures would be reasonably likely to resolve the matter satisfactorily and correspondingly whether countermeasures would aggravate it.[111] If the latter, amicable settlement would presumptively be required.

105 Articles on State Responsibility, *supra* note 13, Article 52(2).

106 Air Services, *supra* note 17, ¶ 91.

107 See *Lac Lanoux* (Fr. v. Sp.) 12 R.I.A.A. 281, 306–07 (Nov. 16, 1957).

108 Kamto, *supra* note 93, at 1171, *citing* commentary to draft article 48, Report of the International Law Commission, 48th Session, 1996 Int'l L. Comm'n YB, vol. II(2), at 69.

109 See, e.g., Luigi Condorelli, La reglement des differends en matiere de responsibilite international des Etats 5 Eur. J. Int'l L. 106 (1994).

110 See, e.g., Bruno Simma, Counter-measures and Dispute Settlement: A Plea for a Different Balance, 5 Eur. J. Int'l L. 102 (1994).

111 See discussion in Iwasawa & Iwatsuki, *supra* note 101, at 1152–53.

4.3 Restrictions on Countermeasures

The law of State responsibility imposes a number of restrictions on the execution of countermeasures. In particular, certain obligations of the injured State may not be breached when conducting countermeasures. These prohibitions apply both to non-cyber responses to internationally wrongful acts carried out by cyber means and to cyber countermeasures taken in response to wrongful acts, whether cyber in nature or not.

Prominent among them is the obligation to refrain from the use of force that is set forth in Article 2(4) of the UN Charter and which reflects customary international law.[112] This prohibition was specifically cited with respect to reprisals in the General Assembly's *Friendly Relations Declaration*.[113] It is also consistent with the ICJ's jurisprudence[114] and is replicated in Article 50(1) of the Articles on State Responsibility.

The dilemma lies in determining when a cyber operation qualifies as a use of force such that it cannot be executed as a countermeasure. No authoritative definition of the term 'use of force' exists in international law. All that is certain is that a cyber operation constitutes a use of force when it is comparable in terms of effects to a non-cyber operations rising to the level of a use of force.[115]

Clearly, a cyber operation that results in damage or destruction of tangible objects or injury or death of individuals beyond a *de minimis* level qualifies. It is also apparent that a cyber operation need not necessarily be physically damaging or injurious to qualify as a use of force. In *Nicaragua*, for example, the ICJ held that the arming and training of guerrillas amounted to a use of force.[116] This conclusion was not based on the attribution of the guerrillas' use of force to the supporting State, but rather on the supporting State's conduct in arming and training them. However, the extent to which activities with consequences falling short physical damage or injury qualify as a use of force remains an unsettled question.

Absent a bright line test for cyber uses of force, the best that can be done at this stage of the law's development is to underline certain non-excusive and extra-legal factors that States are likely to consider when determining whether to characterise a cyber operation as a use of force: immediacy, directness, invasiveness, measurability of effects, military

112 Articles on State Responsibility, supra note 13, Article 50(1)(a). See also *Arbitral Tribunal Constituted Pursuant to Article 287, and in accordance with Annex VII, of the United Nations Convention on the Law of the Sea* (Guy. v. Surin.), Award, ¶ 446 (Perm. Ct. Arb. 2007), http://www.pca-cpa.org/showfile.asp?fil_id=664.

113 Friendly Relations Declaration, *supra* note 45, ¶ 6. *See also* Conference on Security and Co-operation in Europe, Final Act, prin. II, Aug. 1, 1975, 14 I.L.M. 1292.

114 Corfu Channel, *supra* note 14, at 35; Nicaragua, *supra* note 1, ¶ 249.

115 Tallinn Manual, *supra* note 1, r. 11.

116 Nicaragua, *supra* note 1, ¶ 228.

character, State involvement, and presumptive legitimacy.[117] Other factors highlighted as relevant include the prevailing political environment, the identity of the attacker and its record of engaging in hostile actions, and the nature of the target.[118] The approach necessitates a case-by-case analysis in which the weight accorded to these and other factors varies depending on the circumstances. Uncertainty will sometimes result over whether a cyber operation taken in response to an internationally wrongful act reaches the use of force level and thereby fails to qualify as a countermeasure.

A minority assert that forceful countermeasures reaching the level of use of force are appropriate in response to an internationally wrongful act that constitutes a use of force, but remains below the armed attack threshold. This approach responds to a paradoxical consequence of limiting countermeasures to non-forceful actions. In *Nicaragua*, the ICJ asserted that the level of force necessary to breach the prohibition on the use of force was lower than that of an armed attack, the condition precedent to using force in self-defence.[119] Although some States, most notably the US, have rejected the Court's position,[120] if such a 'gap' between uses of force and armed attack thresholds exists, States subjected to uses of cyber force not reaching the armed attack level may only respond with non-forceful actions.

To remedy this situation, Judge Simma, in his separate opinion in the *Oil Platforms* case, has suggested:

> But we may encounter also a lower level of hostile military action, not reaching the threshold of an "armed attack" within the meaning of Article 51 of the United Nations Charter. Against such hostile acts, a State may of course defend itself, but only within the more limited range and quality of responses (the main difference being that the possibility of collective self-defence does not arise, cf. *Nicaragua*) and bound to necessity, proportionality and immediacy in time in a particular strict way.[121]

The reference to the inadmissibility of collective action, which, in part, distinguishes countermeasures from self-defence, confirms that Judge Simma supports a limited right to take forceful countermeasures in the face of a use of force falling within the gap. What this approach might mean in the cyber context will remain an open question until uncertainty as to the use of force and armed attack thresholds is resolved.

---

117 This approach was originally set out in Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885. (1999). It was adopted and adapted in Tallinn Manual, *supra* note 1, at 48–51.

118 *Id*., at 51–52.

119 The Court distinguished 'the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.' Nicaragua, *supra* note 1, ¶ 191. *See also* Oil Platforms, *supra* note 1, ¶ 51; *Armed Activities on the Territory of the Congo* (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, ¶ 147 (Dec. 19).

120 Koh Statement, *supra* note 72, at 7.

121 Oil Platforms, *supra* note 1, Separate Opinion of Judge Simma, ¶ 13.

For States that reject the notion of a gap, this dilemma does not present itself. A State subjected to a wrongful use of force has, by the no-gap interpretation, equally been the object of an armed attack. It may respond with its own use of force, whether cyber or non-cyber in nature, pursuant to the law of self-defence.

Beyond the prohibition on countermeasures involving the use of force, Article 50(1) of the Articles on State Responsibility provides that countermeasures may not affect obligations intended for the protection of fundamental human rights.[122] Although the article does not define the term 'fundamental,' at a minimum it encompasses human rights that may not be derogated from during periods of national emergency or armed conflict.[123] The open question is the degree to which the prohibition extends to other human rights. For instance, cyber activities raise concerns regarding communication and data protection rights,[124] thereby begging the question of whether a cyber operation that violates such rights can qualify as a countermeasure.

In its explication of Article 50(1), the *Commentary* to the Articles on State Responsibility refers to General Comment 8, issued by the UN Committee on Economic, Social, and Cultural Rights.[125] Comment 8, which addresses economic sanctions and their effects on civilians, emphasises that 'it is essential to distinguish between the basic objective of applying political and economic pressure upon the governing elite of a country to persuade them to conform to international law, and the collateral infliction of suffering upon the most vulnerable groups within the targeted country.'[126] The *Commentary* also points to other provisions of international law designed to protect the civilian population, such as international humanitarian law's prohibition on starvation, and the provision in the UN human rights covenants on depriving a people of their means of subsistence.[127] As these references illustrate, there appears to be a general predisposition against countermeasures that might affect the civilian population, as distinct from those designed to coerce the government into compliance with its international legal obligations. There is no rationale for distinguishing cyber from non-cyber countermeasures in this regard.

---

122 Articles on State Responsibility, *supra* note 13, Article 50(1)(b).

123 For instance, see the list of non-derogable rights set forth in Article 4(2) of the *International Covenant on Civil and Political Rights*, Dec. 19, 1966, 999 U.N.T.S. 171.

124 See, e.g., Articles 7 & 8 of the *Charter of Fundamental Rights of the European Union*, Dec. 7, 2000, 2000 O.J. (C 364) 1; Article 8 of the *Convention for the Protection of Human Rights and Fundamental Freedoms*, Nov. 4, 1950, 213 U.N.T.S. 221.

125 Articles on State Responsibility Commentary, *supra* note 28, at 289, *citing* Committee on Economic, Social and Cultural Rights, General Comment 8, The Relationship Between Economic Sanctions and Respect for Economic, Social and Cultural Rights (Seventeenth session, 1997), UN Doc. E/C.12/1997/8 (1997).

126 General Comment 8, *supra* note 125, ¶ 8.

127 Articles on State Responsibility Commentary, supra note 28, at 289–90, citing Article 54(1) of the *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, June 8, 1977, 1125 U.N.T.S. 3; Article 1(2) of the *International Covenant on Civil and Political Rights*, supra note 123; Article 1(2) of the *International Covenant on Economic, Social and Cultural Rights*, Dec. 16, 1966, 993 U.N.T.S. 3.

Article 50(1)(c) also bans the use of belligerent reprisals that are unlawful under international humanitarian law as countermeasures.[128] The *Commentary* to the provision cites the ban on reprisals set forth in the 1929 Geneva Convention, the four 1949 Geneva Conventions, and the 1977 Additional Protocol I to the Geneva Conventions.[129] There is wide agreement that the five referenced Geneva Conventions' prohibitions reflect customary international humanitarian law, and that therefore reprisals (and by extension countermeasures) that target the wounded, sick, shipwrecked, medical personnel, religious personnel and prisoners of war during times of armed conflict are impermissible. For example, it would be forbidden to conduct cyber attacks against the enemy's wounded personnel by cutting electricity to a medical facility in a manner that affected treatment in response to a kinetic or cyber attack on one's own wounded soldiers.

It should be cautioned that some States, including the US, take the position that Additional Protocol I's prohibition on reprisals against civilians is not customary in nature and therefore applies only to States party to that instrument.[130] There being no bar to such reprisals for these States, a cyber reprisal against the civilian population is not unlawful and therefore would not have to qualify as a countermeasure before being conducted. The net result of these positions is that no belligerent reprisal is ever a countermeasure, either because it is subject to a specific exclusion in the law of State responsibility, or because it is lawful and accordingly does not meet the definition of a countermeasure.

States are proscribed from breaching certain other obligations on the basis that they are engaging in countermeasures. Those involving a violation of a peremptory norm, such as genocide, are not permitted.[131] Thus, using cyber or non-cyber means to incite genocide, for instance by manipulating the content of news reports, cannot qualify as a countermeasure. Additionally, as a general matter, cyber or non-cyber countermeasures may not be taken when the obligation that would be violated (whether by an act in cyber space or not) by the countermeasures is subject to a dispute settlement procedure related

128 Articles on State Responsibility, *supra* note 13, Article 50(1)(c).

129 Article 2 of the *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field*, July 27, 1929, 118 L.N.T.S. 303; Article 46 of the *Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, August 12, 1949, 75 U.N.T.S. 31; Article 47 of the *Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, August 12, 1949, 75 U.N.T.S. 85; Article 13 of the *Convention (III) Relative to the Treatment of Prisoners of War*, August 12, 1949, 75 U.N.T.S. 135; Article 33 of the *Convention (IV) Relative to the Protection of Civilian Persons in Time of War*, August 12, 1949, 75 U.N.T.S. 287; Articles 20, 51(6), 52(1), 53(c), 54(4), 55(2), 56(4) of the Additional Protocol I, supra note 127. See also Article 3 of the *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices* (Protocol II), Oct. 10, 1980, 1342 U.N.T.S. 168.

130 *See, e.g.*, Commander's Handbook, *supra* note 35, ¶ 6.2.4.

131 Articles on State Responsibility, *supra* note 13, Article 50 (1).

to the dispute in question.[132] This is so even when the dispute resolution mechanism is contained in the treaty that the responsible State has breached.[133] Countermeasures infringing diplomatic or consular inviolability are also proscribed.[134] As an example, cyber operations directed against an embassy's computer system or that intercept encrypted diplomatic communications cannot qualify as countermeasures. This prohibition includes situations in which the precipitating internationally wrongful act to which the countermeasure would respond was committed by a member of the diplomatic service or otherwise involves the abuse of diplomatic privileges.[135] Of course, States may always agree among themselves to exclude the possibility of countermeasures, usually by means of a treaty provision to the effect that countermeasures are unavailable with respect to the subject matter of the treaty or in certain circumstances set forth in the treaty.[136]

4.4 Proportionality

Countermeasures must, as reflected in Article 51 of the Articles on State Responsibility, be proportionate, that is 'commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.'[137] This principle was set forth in the 1928 *Naulilaa* arbitration: 'Even if one were to admit that the law of nations does not require that the reprisal should be approximately in keeping with the offense, one should certainly consider as excessive and therefore unlawful reprisals out of all proportion to the act motivating them.'[138] A countermeasure that is disproportionate to the injury suffered amounts to punishment or reprisal and is therefore contrary to the object and purpose of the law governing countermeasures. Consequently, its wrongfulness is not precluded.

Proportionality in the context of countermeasures must be distinguished from *jus ad bellum* proportionality, which refers to the amount of force required for a State to effectively defend itself against an armed attack.[139] In some self-defence situations,

---

132 *Id.*, Article 50(2)(a).

133 *Appeal Relating to the Jurisdiction of the ICAO Council* (India v. Pak.), 1972 I.C.J. 46, ¶ 16 (18 Aug.).

134 Articles on State Responsibility, *supra* note 13, Article 50(2)(b). *See also* Tehran Hostages, *supra* note 31, ¶¶ 61–62, 77, 86; Articles 33, 35 of the *Vienna Convention on Consular Relations*, Apr. 24, 1963, 596 U.N.T.S. 261.

135 As the ICJ noted in the *Tehran Hostages* case, diplomatic law is a 'self-contained regime'. Tehran Hostages, *supra* note 31, ¶ 86.

136 *See, e.g.*, *Case C5/94*, R. v. M.A.F.F., *ex parte* Hedley Limited (Ireland), 1996 R.C.R. I-2553.

137 Articles on State Responsibility, *supra* note 13, Article 51; Gabcikovo-Nagymaros Project, *supra* note 14, ¶ 85. For a critical analysis of the subject, see Thomas M. Franck, *On Proportionality of Countermeasures in International Law*, 102 Am. J. Int'l L., 738–42 (2008).

138 Naulilaa, *supra* note 17, at 1028 ('*Même si l'on admettait que le droit des gens n'exige pas que la représaille se mesure approximativement à l'offense, on devrait certainement considérer, comme excessives et partant illicites, des représailles hors de toute proportion avec l'acte qui les a motivées.*').

139 On the requirements of proportionality and necessity in the jus ad bellum context, see Nicaragua, *supra* note 1, ¶¶ 176, 194; Nuclear Weapons, *supra* note 1, ¶ 41; Oil Platforms, *supra* note 1, ¶¶ 43, 73–74, 76. *See also* the

only measures that are disproportionate to the intensity and scope of the precipitating armed attack will suffice to pressure the attacking State into desisting; such measures are generally lawful. Proportionality in the law of self-defence equally limits a State's defensive measures to those that are required to defeat the armed attack, even if they fall short of the intensity of the armed attack that precipitated them.

By contrast, a countermeasure that is out of proportion to the injury suffered is impermissible, even if only action of that intensity and scope would suffice to convince the responsible State to desist in its internationally wrongful conduct. Additionally, a countermeasure may permissibly exceed the minimum intensity and scope necessary to force the responsible State into compliance with its legal obligation to the injured States, so long as it complies with the requirements of purpose and proportionality.[140] In this regard, there is no procedural requirement that the injured State take measures to mitigate damage before taking countermeasures. Nor does the lack of mitigation affect the proportionality of the countermeasures in question. However, the absence of mitigation by the injured State may bear on the calculation of damages for which the originator State is ultimately held responsible.

Countermeasures proportionality must also be distinguished from the concept of proportionality in international humanitarian law, which prohibits an attack during an armed conflict when the expected collateral damage is excessive relative to the anticipated military advantage likely to result.[141] Thus, whereas proportionality in humanitarian law considers the harm caused by the attack in light of the military gain, proportionality in the context of countermeasures gauges harm relative to the injury suffered. In other words, the focus of the former is on the military benefit gained, while that of the latter is on the injury suffered by the State taking the countermeasure.

Subsequent decisions have adopted a slightly broader approach than that articulated in *Naulilaa*, one that dictates consideration of the right involved, a notion incorporated textually in Article 51 of the Articles on State Responsibility. By this approach, appraisal of proportionality is not merely a matter of quantitative comparison of consequences. The *Air Services* Arbitral Tribunal explained,

> [...] it is essential, in a dispute between States, to take into account not only the injuries suffered by the companies concerned but also the importance of the questions of principle arising from the alleged breach. The Tribunal thinks that it will not suffice, in the present case, to compare the losses suffered by Pan Am on account of the suspension of the projected services with the losses which the French companies would have suffered as a result of the counter-measures; it will

discussion in Tallinn Manual, *supra* note 1, at 61-63.

140 For an argument that this should not be the case, see Enzo Cannizzaro, *The Role of Proportionality in the Law of Countermeasures*, 12 Eur. J. Int'l L. 889 (2001).

141 Additional Protocol I, *supra* note 127, Articles 51(5)(b), 57(2)(a)(iii) & 57(2)(b).

> also be necessary to take into account the importance of the positions of principle which were taken when the French authorities prohibited changes of gauge in third countries. If the importance of the issue is viewed within the framework of the general air transport policy adopted by the United States Government and implemented by the conclusion of a large number of international agreements with countries other than France, the measures taken by the United States do not appear to be clearly disproportionate when compared to those taken by France. Neither Party has provided the Tribunal with evidence that would be sufficient to affirm or reject the existence of proportionality in these terms, and the Tribunal must be satisfied with a very approximative appreciation.[142]

The Tribunal therefore concluded that 'judging the "proportionality" of countermeasures is not an easy task and can at best be accomplished by approximation.'[143]

To illustrate, consider the case of countermeasures that affect the interoperability of the responsible State's cyber communications systems. Not only will those effects factor into the proportionality assessment, but so too will the general principle in State practice that cyber communications systems should be operative across borders. The ICJ confirmed this approach in *Gabcikovo-Nagymaros* nearly five decades after the arbitral decision in *Air Services*.[144]

The interconnected and interdependent nature of cyber systems may render it difficult to accurately determine the degree of damage that a countermeasure will likely cause. States will therefore have to exercise due care in assessing whether their actions will be proportionate to the injury suffered and principle involved. This may require, for instance, mapping the targeted system. Since due care is a contextual standard influenced by such factors as the severity of the harm suffered, the extent of further damage caused by any delay, the cyber capabilities of the injured State, and the responsible State's vulnerabilities, it must be determined on a case-by-case basis.

Proportionality does not imply reciprocity; there is no requirement that the injured State's countermeasures breach the same obligation violated by the responsible State. Nor is there any requirement that the countermeasures be of the same nature as the underlying internationally wrongful act that justifies them. Non-cyber countermeasures may be used in response to a wrongful act involving cyber operations, and vice-versa. However, as a general matter, the requirement of proportionality is less likely to be

142 Air Services, *supra* note 17, ¶ 83.

143 *Id*.

144 Gabcikovo-Nagymaros Project, *supra* note 14, ¶¶ 85–87. In doing so, the Court looked to the Permanent Court of Justice's judgment in *Territorial Jurisdiction of the International Commission of the River Oder*, 1929 P.C.I.J. (ser. A-No. 23) No. 16, at 27 (Sept. 10). The Tallinn Manual suggests that *Naulilaa* and *Gabcikovo-Nagymoros* are different standards and that neither has yet achieved prominence. Tallinn Manual, *supra* note 1, at 38–39. The better view is that the latter builds on the former.

breached, or at least to be assessed as having been breached, when the countermeasure is in kind.[145]

There is also no requirement for numerical congruency. A single internationally wrongful act by a responsible State may be responded to by countermeasures that would otherwise breach numerous obligations. An injured State may respond, for instance, to a single wrongful act with a series of different cyber countermeasures, none of which alone would be sufficient to impel the responsible State to desist, but which when combined would do so. The sole question in such a case is whether the combined countermeasures are proportionate to the injury suffered.

4.5 Evidentiary Considerations

Since countermeasures represent a form of self-help, the injured State will typically make the determination as to whether an international obligation has been breached and identify the breach's author. In the event that its assessment 'turns out not to be well-founded,' the injured State's action cannot qualify as a countermeasure.[146] The wrongfulness of the purported countermeasure would not be precluded and the injured State would itself incur responsibility for its response (and be subject to countermeasures).

It is often difficult to attribute cyber activities to a particular State or actor with unqualified certainty. In particular, cyber operations can, as noted, be designed to mask or spoof the originator. As an example, a State may take control of another State's cyber infrastructure and use it to mount harmful operations against a third State to make the injured State conclude that the second State is responsible for them. The *Commentary* to the Articles on State Responsibility, citing the Iran-United States Claims Tribunal, has suggested that the standard for factual attribution is identification with 'reasonable certainty.' [147] This standard would apply both to the identity of the originator and its association with a particular State. A cyber countermeasure undertaken in a mistaken, but reasonable, belief as to the identity of the originator or place of origin would be lawful so long as all other requirements for countermeasures have been met.

The reasonable certainty standard is no less relevant to omissions; States have a duty to stop harmful cyber activities emanating from their cyber infrastructure. In some cases, it may be impossible to attribute a cyber operation with reasonable certainty to a particular State, yet reasonable certainty may have been achieved regarding the location(s) from which the attack has been launched. Should this be so, countermeasures might be appropriate against the State in question for its internationally wrongful failure

145 Articles on State Responsibility Commentary, *supra* note 28, at 285–86.

146 *Id*. at 285.

147 *Id*. at 91, *citing Kenneth P. Yeager v. The Islamic Republic of Iran*, 17 Iran–U.S. Cl. Trib. Rep. 92, 101–02 (1987).

to control cyber activities on its territory, albeit not based on attribution of the activities to that State.

4.6 Originator and Target of Countermeasures

Countermeasures are a tool reserved exclusively to States. They provide no legal basis under international law for a private company, such as an IT firm, to act on its own initiative in response to a harmful cyber operation. This is the case even if such entities possess cyber capabilities that are robust or even exceed those of States. Thus, when Google reportedly 'hacked back' in response to penetration of the company's system by the 'Elderwood Gang,' the operation could not be characterised as a countermeasure even though the group may have had ties to the Chinese government.[148]

However, there is no prohibition on injured States turning to private companies, including foreign companies, to conduct operations on their behalf against responsible States.[149] Of course, the injured State would bear responsibility for the company's actions pursuant to the rules of attribution discussed above. Additionally, a company conducting the cyber operations would be bound by all relevant restrictions and conditions on countermeasures. Failure of the company to abide by them would preclude qualification of the operations as lawful countermeasures; in certain circumstances, it would also generate State responsibility for the company's actions.

Only injured States may engage in countermeasures.[150] Two exceptions to this general principle exist. Pursuant to the Article 48(1) of the Articles on State Responsibility, '[a] ny state other than an injured State is entitled to invoke the responsibility of another state [...] if (a) the obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or (b) the obligation breached is owed to the international community as a whole.'[151] Subparagraph (a) refers to an obligation that is of a collective nature, as in a regional nuclear-free zone treaty. Subparagraph (b) situations generally involve obligations *erga omnes*.[152] Examples of

148 David E. Sanger & John Markoff, *After Google Stand on China, U.S. Treads Lightly,* N.Y. Times, Jan. 14, 2010, http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology&_r=0.

149 On this issue, see Zach West, Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback, 63 Syracuse L. Rev. 119 (2012).

150 Nicaragua, *supra* note 1, ¶ 249.

151 Articles on State Responsibility, *supra* note 13, Article 49(1). Care must be taken to ensure the duty is an obligation in question is not merely hortatory in nature. For instance, the Final Acts of the World Conference on International Telecommunications at Dubai in 2012, which updated the International Telecommunications Regulations, imposes a hortatory duty on member States to 'individually and collectively endeavor to ensure the security and robustness of international telecommunications networks in order to achieve effective use thereof, as well as to the harmonious development of international telecommunications services offered to the public.' Available at http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf. Although the obligation is owed to all members of the organization, none of the members may individually enforce it via countermeasures.

152 On *erga omnes* obligations, see *Barcelona Traction, Light and Power Company, Limited* (Belg. v. Spain), 1970 I.C.J. 3, ¶ 33 (Feb. 5).

the latter include the prohibitions on aggression, genocide, and slavery.[153] Acting on either of these two bases is subject to numerous restrictions.[154]

States may not engage in countermeasures on behalf of another State. The ICJ addressed this issue in the *Nicaragua* case, where it noted that '[t]he acts of which Nicaragua is accused, even assuming them to have been established and imputable to that State, could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts [...]. They could not justify countermeasures taken by a third state [...].'[155] Although there are a few examples of States other than those injured taking actions that would appear to be countermeasures, particularly with respect to economic sanctions,[156] the *Commentary* to the Articles on State Responsibility finds the State practice insufficient to support a norm allowing one State to engage in countermeasures on behalf of another.[157] This is a particularly important restriction in the context of both internationally wrongful cyber acts and cyber countermeasures, for it precludes an injured State that lacks the technical capabilities to engage in cyber countermeasures from seeking the assistance of States possessing them.

Countermeasures may not be 'directed' against States other than the responsible State. In particular, a countermeasure conducted by one State against another that breaches a legal obligation owed by the former to a third State remains wrongful *vis-à-vis* the third State.[158] For instance, a cyber countermeasure that blocks the traffic of the responsible State's private banking system might also negatively impact third States in a fashion that breaches obligations owed to those third States. The fact that the actions qualify as a countermeasure *vis-à-vis* the responsible State does not preclude its wrongfulness as to the others. In light of the networking of cyber systems across borders, the possibility of effects reverberating throughout transborder networks can be high. When this occurs, the question is whether those effects violate legal duties owed to other States in which they manifest.

As illustrated in the aforementioned example, the targets of the countermeasures need not be State organs or State cyber infrastructure, although States must be the 'object' of the countermeasures. In the example, assume that organs of the responsible State

153 *Id.*, ¶¶ 32, 34. *See also East Timor* (Port. V. Austl.), 1995 I.C.J. 90, ¶ 29 (June 30) (self-determination).

154 Articles on State Responsibility Commentary, *supra* note 28, at 276–78.

155 Nicaragua, *supra* note 1, ¶ 249.

156 For instance, following the 1990 invasion of Kuwait by Iraq, a number of States, including US, froze Iraqi assets. Exec. Order No. 12722, Aug. 2, 1990, 55 FR 31803 (1990). *See also* examples set forth at Articles on State Responsibility Commentary, *supra* note 28, at 302–04.

157 Articles on State Responsibility Commentary, *supra* note 28, at 305. Views on the subject appeared to evolve over the course of the deliberations of the International Law Commission. *See* Linos-Alexandre Sicilianos, *Countermeasures in Response to Grave Violations of Obligations Owed to the International Community*, in The Law of International Responsibility, *supra* note 93, at 1137.

158 Articles on State Responsibility Commentary, *supra* note 28, at 285. *See also, e.g., Corn Products International v. Mexico*, Decision on Responsibility, ICSID Case No. ARB(AF)/04/05 (Jan. 15, 2008).

are conducting intrusions to alter data to precipitate a loss of confidence in the injured State's private banking system. The injured State responds in kind. Since the responsible State has itself engaged in an internationally wrongful act, the cyber countermeasure is appropriate; the State is the object of the countermeasure, which is designed to put an end to its wrongful activity. On the other hand, assume that a private firm in the first State is engaging in harmful cyber operations against a competitor in the second State. In such a case, it would be inappropriate to launch countermeasures against the firm unless its action could be attributed to the first State or that State has wrongfully failed to control the activities of the bank.

4.7 Location of Countermeasures

The location from which a cyber countermeasure is launched by an injured State does not bear on its lawfulness. Of course, if launched from a third State, the activity may violate obligations owed to that State, but that fact would not preclude it from qualifying as a lawful countermeasure with respect to the responsible State. Additionally, the lawfulness of a cyber countermeasure against the responsible State is not affected by the location of cyber infrastructure through which it passes (again, in the absence of a specific obligation to the contrary). After all, countermeasures are lawful in nature, even though they would have been unlawful but for the underlying conduct of the responsible State. This is so even when the territory of a third State is involved because the countermeasure is not 'harmful' as a matter of law, and, therefore, does not implicate the obligation to take action to terminate harmful activities emanating from that State's territory. Of course, if allowing the cyber countermeasure to be launched from, or through, the third State's territory would violate another specific obligation the third State owed the responsible State, such as a mutual cyber security agreement, the acquiescence would constitute an internationally wrongful act.

5. Conclusion

The prevailing sense that States stand defenceless in the face of malicious cyber activities that do not qualify as 'armed attacks' endangers international peace and security. In particular, it incentivises treating such operations as armed attacks in order to justify a response by the injured State. Since an armed attack opens the door to forceful defensive reactions, the likelihood of escalation is thereby exacerbated.

This unfortunate perception is not merely destabilising; it is counter-normative. Countermeasures offer States a viable, and lawful, means of responding to harmful cyber actions in a manner more robust than retortion, but less provocative than a use of force. With countermeasures, States will seldom be left with a choice between ineffective response and overreaction.

However, countermeasures are no panacea. They are subject to important restrictions. Most significant among these is the limitation of countermeasures, in contrast to actions in self-defence, to internationally wrongful acts attributable to States. Thus, in the case of cyber operations launched by non-State actors, the international wrongfulness of an injured State's response will not be precluded unless a separate breach by the State to which the injured State's obligations are owed can be identified. In such a case, proportionality will be measured against that breach, not the severity of the non-State actor's operations.

A related restriction is that only States may take countermeasures. Private entities such as IT companies may possess the capability to launch effective countermeasures to protect themselves, but they may not employ them for that purpose except at the behest of a State and in order to enforce an obligation owed to that State by another State under international law. This is a particularly problematic constraint for major multinational corporations operating from States that lack the technical wherewithal to effectively respond to cyber activities directed at cyber infrastructure on their territory.

The limitation to unilateral action further restricts the potential effectiveness of countermeasures. In many cases, the injured State may be unable to respond, yet may enjoy friendly relations with other States that possess the means to do so, and that would be willing to come to the former's assistance. Yet, unlike collective defence, the law of State responsibility does not admit of collective countermeasures. Other restrictions, such as proportionality and purpose, further temper the scope of the resort to countermeasures.

Finally, the restriction of countermeasures to non-forceful actions presents a particular problem in the cyber context. It has the consequence of leaving a State facing cyber uses of force that do not rise to the armed attack level unable to respond in kind. The uncertainty as to where the two thresholds lie with respect to cyber operations complicates matters.

This conundrum is likely to lead to one of two results. One possibility is that States will embrace Judge Simma's position in the *Oil Platforms* case, so as to be able to respond to unlawful cyber uses of force with their own forceful cyber operations not reaching the armed attack level. Of course, such a norm would apply equally in the non-cyber context, thereby removing the speed bump between countermeasures and forceful action represented by the use of force-armed attack gap. Alternatively, States could adopt the US approach, by which all uses of force qualify as armed attacks against which the injured State may respond forcefully. While this would give States a means of responding effectively to cyber uses of force that would otherwise not reach the armed attack level, it would, like the first approach, weaken the conditions precedent for employing force. This might be particularly problematic for States like the US that wield significant cyber capabilities, for it would open the door to forceful responses to their operations.

Despite these limitations, it is clear that the existence of countermeasures as a response option to internationally wrongful cyber acts enables injured States to safeguard their interests without unnecessarily risking escalation. Moreover, the fact that countermeasures may be taken by cyber means widens the range of response options in the face of non-cyber internationally wrongful acts. The greater the range and scope of possible responses, assuming they are properly and wisely employed, the less likely a situation involving international tension is to deteriorate further. States would be well advised to carefully consider the prospects for using countermeasures and to begin developing procedures and rules of engagement for their employment.

Bibliography

Books, Articles and other Publications

Abramovsky A, 'Multilateral Conventions for the Suppression of Unlawful Seizure and Interference with Aircraft Part II: The Montreal Convention' (1975) 14 *Columbia Journal of Transnational Law* 268

Abreu E, 'Cyberattack Reveals Cracks in U.S.' *PCWorld* (9 May 2001) <http://www.pcworld.com/article/49563/article.html>

Akande D and Williams S, 'International Adjudication on National Security Issues: What Role for the WTO?' (2003) 43 *Virginia Journal of International Law* 365

Alexandroff A, 'Challenges in Global Governance: Opportunities for G-x Leadership' (Policy Analysis Brief, The Stanley Foundation 2010)

Alford RP, 'The Self-Judging WTO Security Exception' (2011) 3 *Utah Law Review* 697

Al-Jazeera 'India and Pakistan in Cyber War' *Al-Jazeera* (4 December 2010) <http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html>

Alland D, 'The Definition of Countermeasures', in Crawford J *et al.* (ed), *The Law of International Responsibility* (Oxford University Press 2010)

Allen PD and Demchak C, 'The Palestinian-Israeli Cyberwar' (2003) 83 *Military Review* 52

Allied Business Intelligence (ABI), 'More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020' *ABI research news* (9 May 2013) <https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne>

Alperovitch D, 'Revealed: Operation Shady RAT' (White Paper, McAfee 2011) <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>

Amerasinghe, CF, *Principles of the Institutional Law of International Organizations* (2d ed, Cambridge University Press 2005)

Anderson MS, *The Rise of Modern Diplomacy: 1450-1919* (Longman Group 1939)

Antolin-Jenkins VM, 'Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?' (2005) 51 *Naval Law Review* 132

Antonopoulos C, *The Unilateral Use of Force by States in International Law* (Sakkoulas 1997)

Appelbaum RP and Robinson WI, *Critical Globalization Studies* (Routledge 2005)

Apvrille A, 'NSA's (and GCHQ) Decryption Capabilities: Truth and Lies' *Fortinet* blog (6 September 2013) <http://blog.fortinet.com/NSA-s--and-GCHQ--Decryption-Capabilities--Truth-and-Lies/>

Arimatsu L, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations' in Czosseck C, Ottis R and Ziolkowski K (eds), *4th International Conference on Cyber Conflict. Proceedings* (NATO CCD COE Publications 2012)

Associated Press, 'Israel foils Syrian cyberattack on water system, security expert claims' *Washington Times* (25 May 2013) <http://www.washingtontimes.com/news/2013/may/25/isreal-foils-syrian-cyberattack-water-system-secur/>

Associated Press, 'New Nuclear Sub Is Said to Have Special Eavesdropping Ability' *New York Times* (20 February 2005) <http://www.nytimes.com/2005/02/20/politics/20submarine.html?_r=0>

Baker CD, 'Tolerance of International Espionage: A Functional Approach' (2003-2004) 19 *American University International Law Review* 1092

Baker JE, 'What's International Law Got To Do With It? Transnational Law and the Intelligence Mission' (2007) 28 *Michigan Journal of International Law* 656

Baldwin DA, *Economic Statecraft* (Princeton University Press 1985)

Bambauer DE, 'Cybersieves' (2009) 59 *Duke Law Journal* 377

Bamford J, 'The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)' *Wired* (15 March 2012) <http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/>

Bannon R and Burnett D, 'Submarine Cable Infrastructure Defense Against Terrorists' (2005) *Sea Technology* (July) 19

Barkham J, 'Information Warfare and International Law on the Use of Force' (2001) 34 *New York University Journal of International Law & Politics* 57

Barlow JP, 'A Declaration of Independence for Cyberspace' (Electronic Frontier Foundation 1996) <http://w2.eff.org/Misc/Publications/John_Perry_Barlow/barlow_0296.declaration.txt>

Barnidge RP, 'States' Due Diligence Obligations with regard to International Non-State Terrorist Organisations Post 11 September 2001: the Heavy Burden that States must bear' (2005) 16 *Irish Studies in International Affairs* 103

Barrie GN, 'Spying – An International Law Perspective' (2008) 9 *Journal of South African Law / Tydskrif vir die Suid-Afrikaanse Reg* (2) 238

Barsotti R, 'Armed Reprisals' in Cassese A (ed), *The Current Legal Regulation of the Use of Force* (Martinus Nijhoff 1986)

Baseley-Walker B, 'Transparency and Confidence-Building Measures an Cyberspace: Towards Norms af Behaviour', in Vignard K (ed), *Confronting Cyberconflict* (UNIDIR Disarmament Forum Series 2011/4)

Bassiouni MC, 'A Functional Approach to General Principles of International Law' (1990) 11 *Michigan Journal of International Law* 768

Baumann CE, *The Diplomatic Kidnappings: A Revolutionary Tactic of Urban Terrorism* (Martinus Nijhoff 1973)

BBC, 'Australian ambassador summoned amid Asia US spying reports' *BBC News* (1 November 2013) <http://www.bbc.co.uk/news/world-asia-24757968>

BBC, 'Government loses Spycatcher battle' *BBC News* (13 October 1988) <http://news.bbc.co.uk/onthisday/hi/dates/stories/october/13/newsid_2532000/2532583.stm>

BBC, 'On This Day: 1967: Supertanker Torrey Canyon hits rocks' *BBC News* (18 March 1973) <http://news.bbc.co.uk/onthisday/hi/dates/stories/march/18/newsid_4242000/4242709.stm>

Becker T, *Terrorism and the States: Rethinking the Rules of State Responsibility* (Hart Publishing 2006)

Beckman R, 'Submarine Cables – A Critically Important but Neglected Area of the Law of the Sea' (7th International Conference on Legal Regimes of Sea, Air, Space and Antarctica, New Delhi, January 2010) <http://cil.nus.edu.sg/wp/wp-content/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables-rev-8-Jan-10.pdf>

Bederman DJ, 'Counterintuiting Countermeasures' (2002) 96 *American Journal of International Law* 817

Beigbeder Y, 'World Health Organization (WHO)' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Benatar M, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1 *Goettingen Journal of International Law* 375

Benedetti M, 'Jurisdiction over Cyberspace: YAHOO! in the French and American Courts' Internet' in Cassese S, Carotti B, Casini L, Macchia M, MacDonald E and Savino M (eds), *Global Administrative Law - Cases, Materials, Issues* (2 edn, IRPA-IILJ 2008)

Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006)

Bennet G, 'Space Nuclear Power' in *Encyclopaedia of Physical Science and Technology* (vol 15, Cambridge 2002)

Benzing M, *Das Beweisrecht vor internationalen Gerichten und Schiedsgerichten in zwischenstaatlichen Streitigkeiten* (Springer 2010)

Bergin C, 'NASA Managers Discuss Fragmentation Risks as UARS Heads Back to Earth' (NASA Spaceflight.com, 2011) <http://www.nasaspaceflight.com/2011/09/nasa-managers-fragmentation-risks-uars-heads-back-earth/>

Bernhardt R (ed), *Encyclopedia of Public International Law* (vol 2, North Holland 1995)

Berridge G, *Diplomacy: Theory and Practice* (3rd ed, Palgrave Macmillan 2005)

Besson S, 'Sovereignty' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Bevins V and Wilkinson T, 'New Snowden documents allege US spying on Brazil, Mexico' *Los Angeles Times* (2 September 2013) <http://articles.latimes.com/2013/sep/02/world/la-fg-wn-ff-snowden-spying-brazil-mexico-20130902>

Beyerlin U, 'Different Types of Norms in International Environmental Law: Policies, Principles, and Rules' in Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Beyerlin U, 'Intervention' in Wolfrum R and Philipp C (eds), *United Nations: Law, Policies and Practice* (vol I, CH Beck 1995)

Beyerlin U, 'Sustainable Development' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Beyerlin U and Grote J, 'Stoutenburg, Environment, International Protection', in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Beyerlin U and Holzer V, 'Conservation of Natural Resources', in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Beyerlin U and Marauhn T, *International Environmental Law* (Hart 2011)

Beyerlin U and Stoutenburg J, 'Environment, International Protection' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Billo C and Chang W, 'Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States' (Institute for Security Technology Studies at Dartmouth College 2004) <http://www.ists.dartmouth.edu/projects/archives/cyber-warfare.html>

Birnhack M, 'Reverse Engineering Informational Privacy Law' (2012) 15 *Yale Journal of Law and Technology* 24

Birnie PW, Boyle AE and Redgwell C, *International Law and the Environment* (3rd ed, Oxford University Press 2009)

Bjorklund AK, 'Emergency Exceptions: State of Necessity and Force Majeure' in Muchlinski P *et al.* (eds), *The Oxford Handbook of International Investment Law* (Oxford University Press 2008)

Blanchard JM F and Ripsman NM, 'A Political Theory of Economic Statecraft' (2008) 4 *Foreign Policy Analysis* 371

Blanchard JMF, Mansfield ED and Ripsman NM, 'The Political Economy of National Security: Economic Statecraft, Interdependence, and International Conflict' (1999) 9 *Security Studies* 1

Blanco EM and Razzaque J (eds), *Globalisation and Natural Resources Law: Challenges, Key Issues and Perspectives* (Edward Elgar 2011)

Blay SKN, 'Territorial Integrity and Political Independence' in Wolfrum R (ed) *The Max Planck Encyclopedia of Public International Law* (Oxford University Press 2012)

Blokker NM, 'Preparing Articles on Responsibility of International Organizations: Does the International Law Commission take International Organizations Seriously? A Mid-term Review', in Klabbers J and Wallendahl A (eds), *Research Handbook on the Law of International Organizations* (Edward Elgar 2011)

Blood CG, 'Holding Foreign Nations Civilly Accountable for Their Economic Espionage Practices' (2002) 42 *IDEA – The Journal of Law and Technology* 228

Blue V, 'Exclusive: ITU "Failed," Says Former Policy Chief' *CNET News* (12 December 2012) <http://news.cnet.com/8301-1023_3-57558819-93/exclusive-itu-failed-says-former-policy-chief/>

Blum YZ, 'The Legality of State Response to Acts of Terrorism' in Netanyahu B (ed), *Terrorism. How the West Can Win* (Farrar, Straus and Giroux 1986)

Böckstiegel KH, Benkö M and Hobe S (eds), *Space Law, Basic Legal Documents* (vol 3, ITU 2012)

Bodansky D, 'Deconstructing the Precautionary Principle', in: Caron DD and Schreiber HN (eds), *Bringing New Law to Ocean Waters* (Law of the Sea Institute, University of California 2004)

Bodansky D, *The Art and Craft of International Environmental Law* (Harvard University Press 2010)

Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Bodansky D, Brunnée J and Hey E, 'International Environmental Law – Mapping the Field', in Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Boer L, 'Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace', (2013) 5 *Amsterdam Law Forum* (3) 4

Bölingen S, *Die Transformation der NATO im Spiegel der Vertragsentwicklung: Zwischen sicherheitspolitischen Herausforderungen und völkerrechtlicher Legitimität* (VDM Verlag 2007)

Bolter JD, *Turing's Man: Western Culture in the Computer Age* (Duckworth 1984)

Boone J, 'Mercenary Hacker Group "Hidden Lynx" Emerges as World's Most Potent Cyber Threat' *GlobalPost* (18 September 2013) <http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/hacker-mercenary-group-china-hidden-lynx-worlds-most-potent-cyber-threat>

Borelli S and Olleson S, 'Obligations Relating to Human Rights and Humanitarian Law' in Crawford J *et al.* (eds), *The Law of International Responsibility* (Oxford University Press 2010)

Bothe M, 'Terrorism and the Legality of Pre-emptive Force' (2003) 14 *European Journal of International Law* 227

Bothe M, 'Völkerrechtliche Verhinderung von Gewalt (*ius contra bellum*)' in Graf Vitzthum W (ed), *Völkerrecht* (De Gruyter 2001)

Bovens M, *The Quest for Accountability* (Cambridge University Press 1998)

Bown CP and Trachtman J, 'Brazil – Measures Affecting Imports of Retreaded Tyres: A Balancing Act' (2009) 8 *World Trade Review* 85

Boyle A, 'Some Reflections on the Relationship of Treaties and Soft Law' (1999) 48 *International and Comparative Law Quarterly* 901

Boyles T, CCNA *Security Study Guide: Exam 640-553* (John Wiley and Sons 2010)

Bradsher K, 'China asks other nations not to release its air data' *New York Times* (2012) <http://www.nytimes.com/2012/06/06/world/asia/china-asks-embassies-to-stop-measuring-air-pollution.html?_r=3&>

Brenner J, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin 2011)

Brenner SW, 'Cybercrime Treaty: Criticisms' (*Cyb3rcrim3*, 16 August 2006) <http://cyb3rcrim3.blogspot.com/2006/08/cybercrime-treaty-criticisms.html>

Brenner SW, 'Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?' (2004) 30 *Rutgers Computer & Technology Law Journal* 1

Brenner SW and Crescenzi AC, 'State-Sponsored Crime: The Futility of the Economic Espionage Act' (2006) 28 *Houston Journal of International Law* 389

Bright M, Vulliamy E and Beaumont P, 'Revealed: US dirty tricks to win vote on Iraq War' *The Guardian / The Observer* (2 March 2003) <http://www.theguardian.com/world/2003/mar/02/usa.iraq>

Brölmann CM, *The Institutional Veil in Public International Law: International Organisations and the Law of Treaties* (Hart 2007)

Bronk C and Tikk-Ringas E, 'The Cyber Attack on Saudi Aramco' *Survival* (April–May 2013)

Brown G and Tullos O 'On the Spectrum of Cyberspace Operations' *Small Wars Journal* (12 December 2012) <http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations>

Brown I and Korff D, *Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online* (Global Network Initiative, July 2012) <https://globalnetworkinitiative.org/content/digital-freedoms-international-law>

Brownlie I, 'International Law and the Use of Force by States Revisited' (2000) 21 *Australian Yearbook of International Law* 21

Brownlie I, *International Law and the Use of Force by States* (Oxford University Press 1963)

Brownlie I, *Principles of Public International Law* (6th ed, Oxford University Press 2003)

Brownlie I, *Principles of Public International Law* (7th ed, Oxford University Press 2008)

Brownlie I, *System of the Law of Nations: State Responsibility* (Clarendon Press 1986)

Bruha T, 'Use of Force, Prohibition of' in Wolfrum R and Philipp C (eds), *United Nations: Law, Policies and Practice* (vol I, CH Beck 1995)

Brunnée J, '*Sic utere tuo ut alienum non laedas*' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 212

Buchanan M, 'How the N.S.A. Cracked the Web' *The New Yorker* (7 September2013) <http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html>

Bull H, *The Anarchical Society: A Study of Order in World Politics* (Columbia University Press 1977)

Buxbaum PA, 'Battling Botnets' (*Military Information Technology,* 20 August 2010)

Bygrave L and Bing J, *Internet Governance: Infrastructure and Institutions* (Oxford University Press 2009)

Cafaggi F (ed*), Enforcement of Transnational Regulation – Ensuring Compliance in a Global World* (Edward Elgar 2012)

Calamita NJ, 'Countermeasures and Jurisdiction: Between Effectiveness and Fragmentation' (2011) 42 *Georgetown Journal of International Law* 233

Caldwell LK, *International Environmental Policy: Emergence and Dimensions* (2nd ed, Duke University Press 1990)

Caltagirone S, *Active Response* (Masters thesis, University of Idaho 2005) <http://www.classstudio.com/scatagi/papers/professional_papers/msthesis/sergioThesis.pdf>

Camilleri V, 'How Small States Influence Diplomatic Practice: A Look at The Fourth Round of Accession Negotiations to the European Union' (Paper presented at the International Conference on the Diploacy of Samll States, 8 February 2007) <http://www.um.edu.mt/arts/studyunit/IRL5017>

Campanelli D, 'Solidarity, Principle of' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Cane P, *Responsibility in Law and Morality* (Hart 2002)

Cannizzaro E, 'The Role of Proportionality in the Law of Countermeasures' (2001) 12 *European Journal of International Law* 889

Carbone SM and de Pepe LS, 'States, Fundamental Rights and Duties' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Carnegie Mellon University, Software Engineering Institute, 'SEI grounds Albania-USAID Effort in CERT' (news, undated) <www.sei.cmu.edu/newsitems/rmm-usaid.cfm>

Carotti B and Casini L, 'A Hybrid Public-Private Regime: The Internet Corporation for Assigned Names and Numbers (ICANN) and the Governance of the Internet' in Cassese S, Carotti B, Casini L, Macchia M, MacDonald E and Savino M(eds), *Global Administrative Law - Cases, Materials, Issues* (2nd edn, IRPA-IILJ 2008)

Carr J, *Mandiant APT1 Report Has Critical Analytic Flaws* (*Jeffrey Carr*, 19 February 2013) <http://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html>

Carter BE, 'Economic Coercion' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Carter L, Burnett D, Drew S, Marle G, Hagadorn L, Bartlett-McNeill D and Irvine N, 'Submarine Cables and the Oceans: Connecting the World' in *UNEP-WCMC Biodiversity Series No. 31* (ICPC/UNEP-WCMC 2009) <http://www.unep-wcmc.org/medialibrary/2010/09/10/352bd1d8/ICPC_UNEP_Cables.pdf>

Casarosa F, 'Transnational Private Regulation of the Internet: Different Models of Enforcement', in Cafaggi F (ed), *Enforcement of Transnational Regulation – Ensuring Compliance in a Global World* (Edward Elgar 2012)

Cassese A (ed), *Realizing Utopia - The Future of International Law* (Oxford University Press 2012)

Cassese A, 'When May Senior State Officials be Tried for International Crimes? Some Comments on the Congo v. Belgium Case.' (2002) 13 *European Journal of International Law* 853

Cassese S, Carotti B Casini L, Macchia M, MacDonald E and Savion M (eds), *Global Administrative Law - Cases, Materials, Issues* (2nd edn, IRPA-IILJ 2008)

Cavelty MD, 'The Militarisation of Cyber-space: Why Less May Be Better' in Czosseck C, Ottis R and Ziolkowski K (eds), *4th International Conference on Cyber Conflict. Proceedings* (NATO CCD COE Publications 2012)

Censer M, 'Amazon Web Services, IBM battle over high-profile CIA cloud contract' *Washington Post* (1 September 2013) <http://articles.washingtonpost.com/2013-09-01/business/41670836_1_amazon-web-services-cloud-computing-federal-agencies>

Centre for Strategic and International Studies, *The Economic Impact of Cybercrime and Cyber Espionage* (Report, July 2013)

Cerf V, 'How the Internet Came to Be' (*Virtual School*, 1993) <http://www.virtualschool.edu/mon/Internet/CerfHowInternetCame2B.html>

Cheng B, *General Principles of Law as Applied by International Courts and Tribunals* (Cambridge University Press 1953)

Cheng B, 'The Labyrinth of the Law of International Carriage by Air' (2001) 50 *Zeitschrift für Luft- und Weltraumrecht* 155

Chernenko Y, 'NATO and the CSTO Approach Security Differently' (*Russia Beyond the Headlines,* 4 April 2012) <http://rbth.ru/politics/2013/04/04/nato_and_csto_approach_security_differently_24633.html>

Chester M, 'The Aftermath of the Airplane Accident: Recovery of Damages for Psychological Injuries Accompanied by Physical Injuries Under the Warsaw Convention' (2000) 84 *Marquette Law Review* 227

Chesterman S, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 *Michigan Journal of International Law* 1072

Choucri N, *Cyberpolitics in International Relations* (MIT Press 2012)

Chul-Jae L and Gwang-Lip M, 'Incheon Airport cyberattack traced to Pyongyang' *Korea JoongAng Daily* (5 June 2012) <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2953940>

Cisco, 'Connections Counter: The Internet of Everything in Motion' *Newsroom* (2013) <http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342>

Clarke RA and Knake R, *Cyber War: The Next Threat to National Security and What to Do About It.* (Ecco Books 2010)

Coffen-Smout S and Herbert GJ, 'Submarine Cables: A Challenge for Ocean Management' (2000) 24 *Marine Policy* 441

Colombos CJ, *The International Law of the Sea* (6th edn, Longman 1967)

Combacau J and Sur S, *Droit International Public* (Montchrestien 2012)

Comfort L, Boin A and Demchak C (eds), *Designing Resilience: Preparing for Extreme Events* (University of Pittsburgh Press 2010)

Condorelli L, 'La reglement des differends en matiere de responsibilite international des Etats'(1994) 5 *European Journal of International Law* 106

Condron SM, 'Getting It Right: Protecting American Critical Infrastructure in Cyberspace' (2007) 20 *Harvard Journal of Law & Technology* 403

Conference of American States, *Declaration of American Principles of the Eighth International Conference of American States* (1938)

Conficker Working Group, 'Conficker Working Group – Lessons Learned Document' (*Conficker Working Group* 2012) <http://www.confickerworkinggroup.org/wiki/>

Constantinou M, *On the Way to Diplomacy* (University of Minnesota Press 1966)

Cornish P, 'The Economic Vulnerabilities of Developed States in a Cybered World' (*Discussion Paper: The Vulnerability of the United Kingdom to Economic Cyber Warfare*, Cityforum Limited, June 2011)

Correll SP, 'Operation: Payback Yielded 37 Days of Total Downtime' *PandaLabs* (22 November 2010) <http://pandalabs.pandasecurity.com/two-month-recap-on-operationpayback/>

Correll SP, 'Tis the Season of DDoS – WikiLeaks Edition' *PandaLabs* (4 December 2010) <http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/>

Corten O, 'Judge Simma's Separate Opinion in the Oil Platforms Case: To What Extent Are Armed 'Proportionate Defensive Measures' Admissible in Contemporary International Law?' in Fastenrath *et al.* (ed), *From Bilateralism to Community Interest. Essays in Honour of Judge Bruno Simma* (Oxford University Press 2011)

Corten O, 'Létat de nécessité peut-il justifier un recours à la force non constitutif d'agression?' (2004) 4 *The Global Community Yearbook of International Law & Jurisprudence* 11

Corten O, 'The Controversies over the Customary Prohibition on the Use of Force. A Methodological Debate' (2005) 16 *European Journal of International Law* 802

Cottier T and Müller JP, 'Estoppel' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Council of Europe, Directorate General of Human Rights and Legal Affairs, *International and Multi-Stakeholder Cooperation on Cross-Border Internet* (Interim Report 2010) <http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%20Interim%20Report.pdf>

Coward M, 'Encryption: will it be the death of DPI?' (*Telecoms,* undated) <http://www.telecoms.com/39718/encryption-will-it-be-the-death-of-dpi>

Cowie J, 'Could It Happen In Your Country?' *Renesys* (30 November 2012) <http://www.renesys.com/2012/11/could-it-happen-in-your-countr/>

Cox A, 'The Cyber Espionage Blueprint: Understanding Commonalities in Targeted Malware Campaigns' (*RSA First Watch, Intelligence Report,* 2013) <https://blogs.rsa.com/wpcontent/uploads/2013/07/BLUEPRINT_WP_0713_final.pdf>

CPA Global, 'ICANN earmarks domains record who is for the scrapheap,' *New Legal Review* (12 July 2013) <http://www.cpaglobal.com/newlegalreview/5558/icann_earmarks_domains_record_>

Crawford J, *Brownlie's Principles of Public International Law* (8th edn, Oxford University Press 2012)

Crawford J, *Second Report on State Responsibility – Addendum 2* (United Nations General Assembly, UN Doc. A/CN.4/498/Add.2, 30 April 1999)

Crawford J, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press 2002)

Crawford J, *Third Report on State Responsibility – Addendum 3* (United Nations General Assembly, UN Doc. A/CN.4/507/Add.3, 18 July 2000)

Crimm NJ, 'Post-September 11 Fortified Anti-Terrorism Measures Compel Heightened Due Diligence' (2005) 25 *Pace Law Review* 203

Crovitz G, 'America's First Big Digital Defeat' *Wall Street Journal* (New York, 16 December 2012) <http://online.wsj.com/article/SB10001424127887323981504578181533577508260.html>

Crovitz G, 'Egypt's Revolution by Social Media' *Wall Street Journal* (New York, 13 February 2011) <http://online.wsj.com/news/articles/SB10001424052748703786804576137980252177072>

Crowdy T, *The Enemy Within. A History of Espionage* (Osprey 2006)

Czosseck C, *An Evaluation of State-level Strategies against Botnets in the Context of Cyber Conflicts* (PhD thesis, Estonian Business School 2012)

Czosseck C, Ottis R and Talihärm AM 'Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security' (2011) 1 *International Journal of Cyber Warfare and Terrorism* 24

Czosseck C, Ottis R and Ziolkowski K (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012)

D'Amato A, 'International Law, Cybernetics, and Cyberspace', in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (US Naval War College 2002) 59

d'Argent P and Susani N, 'United Nations, Purposes and Principles' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

d'Aspremont J, 'Abuse of the Legal Personality of International Organizations and the Responsibility of Member States' (2007) 4 *International Organizations Law Review* 91

Damrosch F, 'Retaliation or Arbitration – or Both? The 1978 United States-France Aviation Dispute' (1980) 74 *American Journal of International Law* 785

de Chazounes L and Campanelli D, 'Neighbour States' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

De Janvry A, *The Agrarian Question and Reformism in Latin America* (Johns Hopkins University Press 1981)

De Schutter O, Eide A, Khalfan A, Orellana M, Salomon M and Seiderman I, 'Commentary to the Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights' (2012) 34 *Human Rights Quarterly* 1084

Deeks A, 'Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense' (2012) 52 *Virginia Journal of International Law* 483

Deibert R, *Black Code: Inside the Battle for Cyberspace* (McClelland & Stewart 2013)

Deibert R, 'The Growing Dark Side of Cyberspace (... and What To Do About It)' (2012) 1 *Penn State Journal of Law and International Affairs* 260

Deibert R, Manchanda A, Rohozinski R, Villeneuve N and Walton G, 'Tracking GhostNet: Investigating a Cyber Espionage Network' in *Information Warfare Monitor*, (Munk Centre 2009) <http://www.nartv.org/mirror/ghostnet.pdf>

Deibert R, Palfrey J, Rohozinski R and Zittrain J, *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (The MIT Press 2012)

del Castillio-Laborde L, 'Equitable Utilisation of Shared Resources' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Delbrück J, 'The International Obligation to Cooperate – An Empty Shell or a Hard Law Principle of International Law? – A Critical Look at a Much Debated Paradigm of Modern International Law' in Hestermeyer HP, König D, Matz-Lück N, Röben V, Seibert-Fohr A, Stoll PT and Vöneky S (eds), *Coexistence, Cooperation and Solidarity. Liber Amicorum Rüdiger Wolfrum* (vol 1, Martinus Nijhoff Publications 2011)

Delio M, 'It's (Cyber) War: China vs. U.S.' *Wired* (30 April 2001) <http://www.wired.com/politics/law/news/2001/04/43437?currentPage=all>

Delupis I, 'Foreign Warships and Immunity for Espionage' (1984) 78 *American Journal of International Law* 67

Demarest GD, 'Espionage in International Law' (1996) 24 *Denver Journal of International Law and Policy* 321

Demchak CC, 'Resilience, Disruption, and a "Cyber Westphalia": Options for National Security in a Cybered Conflict World' in Burns N and Price J (eds), *Securing Cyberspace: A New Domain for National Security* (The Aspen Institute 2012)

Demchak CC, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (University of Georgia Press 2011)

Demchak CC and Dombrowski PJ, 'Rise of a Cybered Westphalian Age' (2011) 5 *Strategic Studies Quarterly* 31

Denning DE, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Arquilla J and D Ronfeldt D (eds), *Networks and netwars: The future of terror, crime, and militancy* (RAND Corporation 2001)

Denning DE, 'Cyber Conflict as an Emergent Social Phenomenon' in Holt T and Schell B (eds), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (IGI Global 2010)

Denza E, Diplomatic law: Commentary on the Vienna Convention on Diplomatic Relations (Clarendon Press 1998)

Der Spiegel, Cyberangriffe: Hacker-Meldepflicht für Unterehmen offenbar vor dem Aus, *Der Spiegel* (online), (5 June 2013) <http://www.spiegel.de/netzwelt/netzpolitik/hacker-meldepflicht-fuer-unternehmen-offenbar-vor-dem-aus-a-903824.html>

Der Spiegel 'Growing Alarm: German Prosecutors to Review Allegations of US Spying' *Spiegel online international* (30 June 2013) <http://www.spiegel.de/international/germany/german-prosecutors-to-review-nsa-spying-allegations-a-908636.html>

Der Standard, 'Österreich überlegt Aufstellung einer 'Freiwilligen Cyberwehr'' *derStandard.at* (28 June 2013) <http://derstandard.at/1339639277027/Oesterreich-ueberlegt-Aufstellung-einer-Freiwilligen-Cyberwehr>

DeSchutter O, 'Human Rights and the Rise of International Organisation: The Logic of Sliding Scales in the Law of International Responsibility', in Jan Wouters *et al.* (eds), *Accountability for Human Rights Violations by International Organisations* (Intersentia, 2010) 51

DiGacomo D 'The End of an Evolution: From Air France v. Saks to Olympic Airways v. Husain – The Term "Accident" under Article 17 of the Warsaw Convention Has Come Full Circle' (2004) 16 *Pace International Law Review* 409

Diggelmann O, 'Militärische Gewalt bei Cyberattacken?' *Neue Zürcher Zeitung* (30 May 2013) <http://www.nzz.ch/aktuell/international/uebersicht/militaerische-gewalt-bei-cyberattacken-1.18089666>

DiMascio N and Pauwelyn J 'Non-discrimination in Trade and Investment Treaties: Worlds Apart or Two Sides of the Same Coin?' (2008)102 *American Journal of International Law* 48

Dinstein Y 'Criminal Jurisdiction over Aircraft Hijacking' (1972) 7 *Israel Law Review* 195

Dinstein Y, 'Computer Network Attack and Self-Defense' in Schmitt NM and O'Donnell BT (eds), *Computer Network Attack and International Law* (US Naval War College 2002)

Dinstein Y, *War, Aggression and Self-Defence* (3rd edn, Cambridge 2001)

DiploFoundation 'Emerging Language of Internet Diplomacy' *Diplo* (Malta, 2013) <http://www.diplomacy.edu/IGFlanguage>

Dittrich D and Himma K, 'Active Response to Computer Intrusions' in Bidgoli H (ed), *The Handbook of Information Security* (Hoboken 2005) 664

Dobbin F, Simmons B and Garrett G, 'The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?' (2007) 33 *Annual Review of Sociology* 449

Dombrowski PJ and Demchak CC, 'Cyber Westphalia: Asserting State Prerogatives in Cyberspace' (2014) *Georgetown Journal of International Affairs* (special issue on cyber)

Donadio R, 'Larger Threat is Seen in Google Case' *New York Times* (24 February 2010) <http://www.nytimes.com/2010/02/25/technology/companies/25google.html?_r=2&pagewanted=all>

Donnelly B and Bishop P, 'Natural Law and Ecocentrism' (2007) 19 *Journal of Environmental Law* 89

Dörr O, 'Use of Force, Prohibition of' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Drezner DW, 'The Hidden Hand of Economic Coercion' (2003) 67 *International Organization* 643

Drucker PF, *The New Realities: In Government and Politics, in Economics and Business, in Society and World View* (Heinemann Professional Publishing 1989)

Dupuy P-M, 'Formation of Customary International Law and General Principles' in: Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Dupuy RJ and Hoss, 'Trail Smelter and Terrorism: International Mechanisms to Combat Transboundary Harm' in Bratspies R and Miller R (eds), *Transboundary Harm in International Law. Lessons from the Trail Smelter Arbitration* (Cambridge 2006)

Dupuy RJ and Vignes D (eds), *A Handbook on the Law of the Sea* (Martinus Nijhoff 1991)

Dworkin R, *Taking Rights Seriously* (Bloomsbury 1977)

EADS, 'Robotic Geostationary Orbit Restorer, Final Report-Executive Summary' (2003) *EADS Space Transportation* 1

Eagleton C, 'International Organization and the Law of Responsibility' (1959/I) 76 *Recueil des Cours* 319

Easterbrook FH, 'Cyberspace and the Law of the Horse' (1996) *University of Chicago Legal Forum* 207

Eaton J and Engers MP 'Sanctions: some simple analytics' (1999) 89 *American Economic Review* 409

Ebrahim E and Weisband E (eds), *Global Accountabilities: Participation, Pluralism, and Public Ethics* (Cambridge University Press 2007)

Economic Times, 'Cyber espionage on the rise, energy assets most vulnerable' *The Economic Times* (Mumbai 31 May 2012) <http://www.sustainabilityoutlook.in/news/cyber-espionage-rise-energy-assets-most-vulnerable>

Economist, 'A walk on the dark side' *The Economist* (30 August 2007) <http://www.economist.com/node/9723768>

Economist, 'Business and cyber-crime: Firewalls and Firefights' *The Economist* (10 August 2013) 47

Edmondson LS, 'Espionage in Transnational Law' (1972) 5 *Vanderbilt Journal of Transnational Law* (2) 444

Elagab O, *The Legality of Non-Forcible Counter-Measures in International Law* (Oxford University Press 1988)

Elkin-Koren N and Salzberger EM, *Law, Economics and Cyberspace. The Effects of Cyberspace on the Economic Analysis of Law* (Edward Elgar 2004)

Emanuelli C, 'The Right of Intervention of Coastal States on the High Seas in Cases of Pollution Casualties' (1976) 25 *University of New Brunswick Law Journal* 79

Emigh J, 'RIM vs. India and Saudi Arabia: Let's Make a Deal on Encrypted Data' *Brighthand* (14 August 2010) <http://www.brighthand.com/default.asp?newsID=16910&news=BlackBerry+Blocked+India+Saudi+Arabia+Agreement+RIMM>

Epping V and Gloria C, 'Der Staat im Völkerrecht' in Ipsen K (ed), *Völkerrecht* (6th edn, CH Beck 2010)

Epping V, Fischer H and Heinschel von Heinegg W (eds), *Brücken bauen und begehen. Festschrift für Knut Ipsen zum 65 Geburtstag* (CH Beck 2000)

Eurocontrol, *Manual for National ATM Security Oversight* (EUROCONTROL, Directorate Single Sky 2012, v.1.0)

European Network of Excellence in Cryptology II, 'ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)' (2012) <http://www.ecrypt.eu.org/documents/D.SPA.20.pdf>

European Union Agency for Network and Information Security, 'Annual Incident Reports' <http://www.enisa.europa.eu/media/press-releases/new-major-incidents-in-2012-report-by-eu-cyber-security-agency-enisa>

European Union Agency for Network and Information Security, 'Proactive Detection of Security Incidents, Honeypots' (Report 2012) <http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots>

European Union, *EU Cybersecurity Plan to protect open internet and online freedom and opportunity*, Press Release No. IP/13/94 (EU 7 February 2013) <http://europa.eu/rapid/press-release_IP-13-94_en.htm>

European Union, European Defence Agency, 'European Harmonized Military Airworthiness Basic Framework Concerning the Development, the Acceptance and the Implementation of European Military Airworthiness Requirements' <http://www.eda.europa.eu/info-hub/news/2013/06/19/european-defence-agency-reflects-on-the-need-for-greater-harmonisation-in-military-airworthiness>

European Union, European Parliament, 'An Appraisal of Technologies of Political Control' (Directorate General for Research, Scientific and Technological Options Assessment, Working Document, PE 166 499, 6 January 1998) <http://cryptome.org/stoa-atpc.htm>

European Union, European Parliament, 'Prism: MEPs hit out at US surveillance of people's personal data' *European Parliament News* (11 June 2013) <http://www.europarl.europa.eu/news/en/headlines/content/20130611STO11522/html/Prism-MEPs-hit-out-at-US-surveillance-of-people's-personal-data>

European Union, European Parliament, 'Q&A on EU Data Protection Reform' *European Parliament News* (22 October 2013) <http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform>

European Union, European Parliament, 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)' (2001/2098(INI), Doc. No. A5-0264/2001 PAR1, 11 July 2001) <http://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_en.pdf>

Evans D, *The Internet of Things. How the Next Evolution of the Internet is Changing Everything* (CISCO IBSG, April 2011) <http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>

Evron G, 'Battling Botnets and Online Mobs' (2008) 9 *Georgetown Journal of International Affairs* 121

Falk RA, 'Space Espionage and World Order: A Consideration of the Samos-Midas Program' in Stanger RJ (ed), *Essays on Espionage and International Law* (Ohio State University Press 1962)

Falliere N, Murchu LO and Chien E, *W32.Stuxnet Dossier Ver 1.3* (Symantec, 2010) <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>

Farer TJ, 'Political and Economic Coercion in Contemporary International Law' (1985) 79 *American Journal of International Law* 405

Farivar C, 'A Brief Examination of Media Coverage of Cyberattacks (2007 - Present)' in Czosseck C and Geers K (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009)

Farwell JP and Rohozinski R, 'Stuxnet and the Future of Cyber War' (2011) 53 *Survival* 23

Fassbender B, 'Die Souveränität des Staates als Autonomie im Rahmen der völkerrechtlichen Verfassung' in Mansel HP, Pfeiffer T, Kronke H, Kohler C and Hausmann R (eds), *Festschrift für Erik Jayme* (vol 2, Sellier 2004)

Fastenrath U, 'Article 74' in Simma B *et al.* (eds), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012)

Federal Republic of Germany, *Cyber-Sicherheitsstrategie für Deutschland* (February 2011) <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile>

Federal Republic of Germany, Ministry for the Interior, *Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* (7 March 2013) <http://bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.html>

Federal Republic of Germany, Ministry of Defence, 'White Paper on German Security Policy and the Future of the Bundeswehr' (2006) <http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/DcLBDYAgDADAWVyg_ftzC_VXsIEGaIlUXF9zhyf-lKYkcjGlijseUdbwQmgzwZCY-c4sPrpVcSlAmjiYM1xWnsbqjL1sywdHoTKR/>

Federal Republic of Germany, Office for Information Security, 'BSI: CIP Implementation Plan' (2007) <https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/ImplementationPlan/implementationplan_node.html>

Ferrazzani M, 'Remote Sensing, General Principles and ESA Policy' *Proceedings of the Third ECSL/Dutch NPOC Workshop* (Noordwijk 1994) 13

Fidler D, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies' (2013) 17 *American Society of International Law Insights* 1 <http://www.asil.org/insights130320.cfm>

Fidler D, 'Was Stuxnet an Act of War? Decoding a Cyberattack' (2011) 9 *IEEE Security and Privacy* 56

Fidler D, 'Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage' (*Arms Control Law Blog*, 11 February 2013) <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

Financial Times 'US warns on German telecoms' *Financial Times* (12 August 1999)

Finkle J, 'Inside a global cybercrime ring' *Reuters* (24 March 2010) <http://www.reuters.com/article/2010/03/24/us-technology-scareware-idUSTRE62N29T20100324>

Fiorita D, 'Aviation Security: International Response' (1993) 3 *Albany Law Journal of Science & Technology* 267

FireEye, 'The Advances Attack Landscape' (*FireEye* Report 2013) <http://www2.fireeye.com/WEB2013ATLReport.html>

Fischer D, 'What is a Botnet? (Botnet Definition)' (*Kasperspy Lab*, 25 April 2013) <http://blog.kaspersky.com/botnet/>

Fischer H, 'Diplomatische und konsularische Beziehungen' in Ipsen K (ed), *Völkerrecht* (6th edn, CH Beck 2010)

Fischer M, 'The three big questions on Syria's Internet blackout' *Washington Post* (29 November 2012) <http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/29/the-three-big-questions-on-syrias-internet-blackout/>

Fisher M 'South Korea under Cyber Attack: Is North Korea Secretly Awesome at Hacking?' *Washington Post* (20 March 2013) <http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/20/south-korea-under-cyber-attack-is-north-korea-secretly-awesome-at-hacking/>

Fisher M and Keller J 'Syria's Digital Counter-Revolutionaries' *The Atlantic* (31 August 2011) <http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/>

Fleck D, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 *Michigan Journal of International Law* 688

Florent C, *Security Issues with DNS* (SANS Institute Reading Room, 2003) <http://www.sans.org/reading-room/whitepapers/dns/security-issues-dns-1069?show=security-issues-dns-1069>

Forcese C, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 *Journal of National Security Law and Policy* 195

Foster CE, 'Necessity and Precaution in International Law: Responding to Oblique Forms of Urgency' (2008) 23 *New Zealand Universities Law Review* 265

Foster CE, *Science and the Precautionary Principle in International Courts and Tribunals* (Cambridge 2011)

France, *Stratégie de la France, Défense et sécurité des systèmes d'information* (2011) <http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011>

France 24, 'Twitter tells the real-time story of the quake's human toll' *France 24* (28 February 2010) <http://www.france24.com/en/20100227-twitter-disaster-info-chile-earthquake-america-south-tsunami-internet>

Franck TM, 'On Proportionality of Countermeasures in International Law' (2008) 102 *American Journal of International Law* 715

Franck TM, *Recourse to Force. State Action against Threats and Armed Attacks* (Cambridge 2002)

Franck TM, 'Reflections on Force and Evidence' (2006) 100 *Proceedings of the American Society of International Law* 51

Franzese PW, 'Sovereignty in Cyberspace: Can It Exist?' (2009) 64 *Air Force Law Review* 1

Fraser N, *Scales of Justice: Reimagining Political Space in a Globalizing World* (Columbia University Press 2009)

Free World Centre, *The Right to Share: Principles on Freedom of Expression and Copyright in the Digital Age* (London, 2013) <http://www.article19.org/data/files/medialibrary/3716/13-04-23-right-to-share-EN.pdf>

Friedmann W, 'The Uses of "General Principles" in the Development of International Law' (1963) 57 *American Journal of International Law* 279

Fritz J 'How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness' (2008) 8 *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies* 1

Frowein JA, '*Ius Cogens*' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Fryer-Biggs Z, 'New Cyber "Mercenaries" Prefer Quick Strikes, Researchers Say' *Defense News* (27 September 2013) <http://www.defensenews.com/article/20130927/DEFREG02/309270009/New-Cyber-Mercenaries-Prefer-Quick-Strikes-Researchers-Say?odyssey=nav%7>

Furnas A, 'Why an international trade agreement could be as bad as SOPA,' *The Atlantic* (6 February 2012) <http://www.theatlantic.com/technology/archive/2012/02/why-an-international-trade-agreement-could-be-as-bad-as-sopa/252552/>

Gaja G, 'General Principles of Law', in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Gale Group, 'Espionage and Intelligence, Early Historical Foundations' *Gale Encyclopedia of Espionage & Intelligence* <http://www.answers.com/topic/espionage-and-intelligence-early-historical-foundations>

Garcia-Mora MR, 'Treason, Sedition and Espionage as Political Offences under the Law of Extradition' (1964) 26 *University of Pittsburgh Law Review* 79

Garner BA (ed), *Black's Law Dictionary* (7th ed, West Group 1999)

Gartzke E and Li Q, 'War, Peace, and the Invisible Hand: Positive Political Externalities of Economic Globalization' (2003) 47 *International Studies Quarterly* 561

GATT Council, 'Minutes of Meeting Held in the Centre William Rappard on Oct. 10, 1985' (Doc. No. C/M/192, 24 Oct. 1985) <http://www.wto.org/gatt_docs/English/SULPDF/91170093.pdf>

GATT Council, 'Summary Record of the Twenty-Second Meeting' (Doc. No. CP.3/SR.22, 8 June 1949) <http://www.wto.org/gatt_docs/English/SULPDF/90060100.pdf>

GATT, 'Panel Report, United States – Trade Measures Affecting Nicaragua' (Doc. No. L/6053, 13 October 1986) <http://www.wto.org/gatt_docs/English/SULPDF/91240197.pdf>

Gaycken S, 'Krieg der Rechner' in (2011) *Internationale Politik* (April) 88

Gaycken S, 'The Necessity of (Some) Certainty – A Critical Remark Concerning Matthew Sklerov's Concept of "Active Defense"' (2010) 12 *Journal of Military and Strategic Studies* 1

Gazzini T, *The Changing Rules on the Use of Force in International Law* (Manchester 2008)

Geers K, 'World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks' (*FireEye Labs*, 24 Sept. 2013) <http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf>

Gehring T, 'Treaty-Making and Treaty Evolution' in Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Gellman B and Poitras L, 'U.S, British intelligence mining data from nine U.S. Internet companies in broad secret program' *Washington Post* (6 June 2013) <http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers>

Gellner E, *Postmodernism, Reason and Religion* (Psychology Press 1992)

Geuss R, *Philosophy and Real Politics* (Princeton University Press 2008)

Gibson W, *Neuromancer* (Ace Books 1983)

Giles K, '"Information Troops" – a Russian Cyber Command?' in Czosseck C, Tyugu E and Wingfield TC (eds), *3rd International Conference on Cyber Conflict. Proceedings* (NATO CCD COE Publications 2011)

Giles K, 'Opinion: Cyber attack on Finland is warning for EU' *Eureporter* (12 November 2013) <http://www.eureporter.co/frontpage/2013/11/12/opinion-cyber-attack-on-finland-is-warning-for-eu/>

Giles K, 'Russia's Public Stance on Cyberspace Issues' in Czosseck C, Ottis R, Ziolkowski K (eds), *4th International Conference on Cyber Conflict. Proceedings* (NATO CCD COE Publications 2012)

Giles K and Hagestad II W, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in Podins K, Stinissen J and Maybaum M (eds), *5th International Conference of Cyber Conflict. Proceedings* (NATO CCD COE Publications 2013)

Gill TD, 'Military Intervention at the Invitation of a Government' in Gill TD and Fleck D (eds), *Handbook of the International Law of Military Operations* (Oxford University Press 2011)

Gill TD, 'The Forcible Protection, Affirmation and Exercise of Rights under Contemporary International Law' (1992) 23 *Netherlands Yearbook of International Law* 105

Gill TD and Ducheine P, 'Anticipatory Self-Defense in the Cyber Context' (2013) 89 *International Law Studies* 438

Gill TD and Fleck D, *Handbook of the International Law of Military Operations* (Oxford University Press 2011)

Gilman N, Goldhammer J and Weber S, *Deviant globalization: Black market economy in the 21st century* (Continuum 2011)

Gini A, 'Safety of Nuclear Powered Missions' *Space Safety Magazine* (21 Oct. 2011) <http://www.spacesafetymagazine.com/2011/10/21/plutonium-power-source-considered-choice-type-deep-space-missions-extraordinary-scientific-results-missions-voyager-pioneer-apollo-nuclear-power-yet-senate-appropriations-committee-decided-fund-ad/>

Ginther K, *Die völkerrechtliche Verantwortlichkeit internationaler Organisationen gegenüber Drittstaaten* (Springer 1969)

GIODO, 35th International Conference of Data Protection and Privacy Commissioners, *Resolution on anchoring data protection and the protection of privacy in international law* (Warsaw, September 2013) <https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf>

Gjelten T, 'Is All The Talk About Cyberwarfare Just Hype?' *GBP News* (15 March 2013) <http://www.gpb.org/news/2013/03/15/is-all-the-talk-about-cyberwarfare-just-hype>

Gladwell M, 'Does Egypt Need Twitter?' *The New Yorker* (New York, 2 February 2011) <http://www.newyorker.com/online/blogs/newsdesk/2011/02/does-egypt-need-twitter.html>

Glennon MJ, *Constitutional Diplomacy* (Princeton University Press 1990)

Glennon MJ, *Limits of Law, Prerogatives of Power: Interventionism after Kosovo* (Palgrave Macmillan 2001)

Glennon MJ, 'The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter' (2002) 25 *Harvard Journal of Law & Public Policy* 539

Glennon MJ, 'The Road Ahead: Gaps, Leaks and Drips' (2013) 89 *International Law Studies* 362

Glennon MJ, 'Why the Security Council Failed' (2003) 82 *Foreign Affairs* 16

Glenny M, *Dark Market* (Random House 2011)

Gobry P-E, 'The Internet is 20% of economic growth' *Business Insider* (24 May 2011) <http://www.businessinsider.com/mckinsey-report-internet-economy-2011-5>

Goldman E, *Power in Uncertain Times: Strategy in the Fog of Peace* (Stanford University Press 2010)

Goldsmith J, 'Against Cyberanarchy' (1998) 65 *University of Chicago Law Review* 1199

Goldsmith J, 'Cybersecurity Treaties: A Sceptical View' (Stanford University, Hoover Institution, Koret-Taube Task Force on National Security and Law 2011) <http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf>

Goldsmith J, 'How Cyber Changes the Laws of War' (2013) 24 *European Journal of International Law* 129

Goncharov M, 'Russian Underground 101' (Trend Micro Research Paper 2012) <http://www.trendmicro.co.nz/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>

Gong X, 'The new development of International Law on Civil Aviation Security: The Beijing Convention and Beijing Protocol of 2010' (2010) 4 *Journal of Eest Asia & International Law* 232

Goodin D, 'Almost 2,500 firms breached in ongoing hack attack: Zeus and Waledac unite in global botnet' *The Register* (18 February 2010) <http://www.theregister.co.uk/2010/02/18/massive_hack_attack/>

Goodin D, 'Upstart crimeware wages turf war on mighty Zeus bot: All your bots belong to us' *The Register* (18 February 2010) <http://www.theregister.co.uk/2010/02/09/spyeye_bots_vs_zeus/>

Gorman S, 'China Hackers Hit U.S. Chamber' *Wall Street Journal* (21 December 2011) A1

Gorman S, Dreazen Y and Cole A, 'Insurgents hack U.S. drones – $26 Software is used to breach Key Weapons in Iraq: Iranian Backing Suspected' *Wall Street Journal Europe* (17 December 2009)

Gorman S and Yadron D, 'Iran Hacks Energy Firms, U.S. Says' *Wall Street Journal* (23 May 2013) <http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968>

Graham B, 'Hackers Attack Via Chinese Web Sites' *Washington Post* (25 August 2008) <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>

Graham D, 'Cyber Threats and the Law of War' (2010) 4 *Journal of National Security: Law & Policy* 87

Green JA, 'Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice' (2009) 58 *International & Comparative Law Quarterly* 163, 166

Green JA, 'Questioning the Peremptory Status of the Prohibition of the Use of Force' (2011) 32 *Michigan Journal of International Law* 215

Green MP and Burnett DR, 'Security of International Submarine Cable Infrastructure – Time to Rethink?' in Nordquist MH, Wolfrum R, Moore JN and Long R (eds), *Legal Challenges in Maritime Security* (Martinus Nijhoff 2008)

Greenberg A, 'Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits' *Forbes* (23 March 2012) <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>

Greenberg LT, Goodman SE and Soo Hoo KJ, *Information Warfare and International Law* (US National Defense University 1998)

Greenwald G and MacAskill E, 'Boundless Informant: the NSA's secret tool to track global surveillance data' *The Guardian* (11 June 2013) <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>

Greenwood C, 'Caroline, The' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Greenwood C, 'International Law and the "War Against Terrorism"' (2002) 78 *International Affairs* 301

Greenwood C, 'Self-Defence' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Gross M, 'Use of Civilians as Human Shields: What Legal and Moral Restrictions Pertain to a War Waged by a Democratic State Against Terrorism?' (2002) *Emory International Law Review* 445

Gross MJ, 'Enter the Cyber-dragon' *Vanity Fair* (September 2011) <http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109>

Gross MJ, 'Stuxnet Worm: A Declaration of Cyber-War' *Vanity Fair* (April 2011) <http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104>

Guilfoyle D, 'Counter-Piracy Law Enforcement and Human Rights' (2010) 59 *International & Comparative Law Quarterly* 141

Haass R, 'The case for messy multilateralism' *Financial Times* (5 January 2010)

Hamill J, 'Osborne to China: Keep watching Downton and we'll gloss over Huawei security worries' *The Register* (14 October 2013) <http://www.theregister.co.uk/2013/10/14/chancellor_to_china_keep_watching_downton_and_well_gloss_over_huawei_security_worries/>

Hamilton K and Langhorne R, *The Practice of Diplomacy* (Routledge 1995)

Hammarskjöld K, 'Air piracy as an international crime: suggestions for international action' (1976) 32 *International Review of Criminal Policy* 14

Handl G, 'Transboundary Impact' in Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Hanson VD, *Carnage and Culture* (Doubleday 2001)

Hanzhang T, *Sun Tzu's Art of War: The Modern Chinese Interpretation* (Sterling Publishing Company 2007)

Hardin G, 'The Tragedy of the Commons' (1968) 162 *Science* 1243

Hare F, 'The Significance of Attribution to Cyberspace Coercion: A Political Perspective' in Czosseck C, Ottis R and Ziolkowski K (eds), *4th International Conference on Cyber Conflict. Proceedings* (NATO CCD COE Publications 2012)

Harland D and Lorenz R, *Space System Failures* (Springer Praxis 2005)

Hart HLA, *The Concept of Law* (Clarendon Press 1961)

Harvard Research in International Law, 'Draft Convention on Jurisdiction with respect to Crime' (1935) 29 *American Journal of International Law* 439

Harvard Research in International Law, 'Jurisdiction with Respect to Crime' (1935) 29 *American Journal of International Law* (Supp) 435

Haryey B, 'What is a Hacker?' (1985) <http://www.cs.berkeley.edu/~bh/hacker.html>

Hassanpour N, 'Media Disruption Exacerbates Revolutionary Unrest: Evidence from Mubarak's Natural Experiment' (APSA Annual Meeting Paper 2011)

Hasslinger KM, 'Undersea Warfare: the Hidden Threat' *Armed Forces Journal* (1 March 2008) <http://armedforcesjournal.com/article/2008/03/3348196>

Hathaway OA *et al,* 'The Law of Cyber Attack' (2012) 100 *California Law Review* 817

Healey J (ed), *A Fierce Domain: Conflict in Cyberspace*, *1986-2012* (Cyber Conflict Studies Association Publication in Partnership with the Atlantic Council 2013)

Heathcote S, 'Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Necessity' in Crawford J *et al.* (ed), *The Law of International Responsibility* (Oxford University Press 2010)

Heathcote S, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility' in Bannelier K *et al.* (eds), *The ICJ and the Evolution of International Law. The Enduring Impact of the Corfu Channel Case* (Routledge 2012)

Heijmans M and Melissen J, 'Foreign Ministries and the Rising Challenge of Consular Affairs: Cinderella in the Limelight' in Rana KS and Kurbalija J (eds), *Foreign Ministries: Managing Diplomatic Networks and Optimizing Value* (DiploFoundation 2007) 192

Heintschel von Heinegg W, 'Die weiteren Quellen des Völkerrechts' in Ipsen K (ed), *Völkerrecht* (6th edn, CH Beck 2010)

Heintschel von Heinegg W, 'Informationskrieg und Völkerrecht. Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung', in Epping V, Fischer H and Heintschel von Heinegg W (eds), *Brücken bauen und begehen. Festschrift für Knut Ipsen zum 65. Geburtstag* (CH Beck 2000) 134

Heintschel von Heinegg W, 'Legal Implications of Territorial Sovereignty in Cyberspace' in C Czosseck, R Ottis and K Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publication 2012) 7ff

Heintschel von Heinegg W, 'Repressing Piracy and Armed Robbery at Sea – Towards a New International Legal Regime?' (2010) 40 *Israel Yearbook on Human Rights* 219

Heintschel von Heinegg W, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 *International Law Studies* 123

Help Net Security, 'Nearly 200,000 new malware samples appear daily' (24 June 2013) <http://www.net-security.org/malware_news.php?id=2521>

Henriksen H, 'Diplomacy and Small States in Today's World' in *The face of man, Vol. 2, The Dr. Eric Williams Memorial Lectures 1993 – 2004* (Trinidad and Tobago, Central Bank of Trinidad and Tobago 2005) <http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3224>

Hess P, 'China prevented repeat cyber attack on US' *United Press International* (29 October 2002) <http://www.upi.com/Business_News/Security-Industry/2002/10/29/China-prevented-repeat-cyber-attack-on-US/UPI-51011035913195/>

Hestermeyer HP, 'Reality or Aspiration? – Solidarity in International Environmental and World Trade Law' in Hestermeyer HP, König D, Matz-Lück N, Röben V, Seibert-Fohr A, Stoll PT and Vöneky S (eds), *Coexistence, Cooperation and Solidarity. Liber Amicorum Rüdiger Wolfrum*, vol 1 (Martinus Nijhoff 2011)

Hestermeyer HP, 'Vienna Convention on Diplomatic Relations (1961)' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Hestermeyer HP, König D, Matz-Lück N, Röben V, Seibert-Fohr A, Stoll PT and Vöneky S (eds), *Coexistence, Cooperation and Solidarity. Liber Amicorum Wolfrum R* (vol 1, Martinus Nijhoff 2011)

Hewlett Packard, 'Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles' (Press Release, 8 October 2012) <http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html>

Hibbert R, *Intelligence and National Security* (Hodder and Stoughton 1990)

Hickey K, 'Dark cloud: Study finds security risks in virtualization' *GCN* (18 March 2010) <http://gcn.com/Articles/2010/03/18/dark-cloud-security.aspx>

Hicks SC, 'International Order and Article 38(1)(c) of the Statute of the International Court of Justice' (1978) 2 *Suffolk Transnational Law Journal* 1

Higgins AP, 'Submarine Cables and International Law' (1921-1922) 2 *British Yearbook of International Law* 27

Higgins P, *Hall's International Law* (8th ed, Halls 1924)

Higgins R, *Problems and Process: International Law and How We Use It* (Oxford University Press 1994)

Hill R, 'WCIT: Failure or Success, Impasse or Way Forward' (2013) 21 *International Journal of Law and Information Technology* 313

Hinkle KC 'Countermeasures in the Cyber Context: One More Thing to Worry About' (2011) 37 *The Yale Journal of International Law* (Online)

Hirsch M, *The Responsibility of International Organizations toward Third Parties: Some Basic Principles* (Martinus Nijhoff 1995)

Hock R, 'Internet Tools and Resources for Open Source Intelligence' *Onstat.com* (13 September 2013) <http://www.onstrat.com/osint/>

Hoisington M, 'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense' (2009) 32 *Boston College International & Comparative Law Review* 439

Holland TE, *The Elements of Jurisprudence* (13th ed, Clarendon Press 1924)

Hollis DB, 'An e-SOS for Cyberspace' (2011) 52 *Harvard Journal of International Law* 397

Honoré T, *Responsibility and Fault* (Hart 1999)

Hou N, 'China to enhance cooperation with ASEAN in cyber security' *CCTV News* (11 September 2013) <http://english.cntv.cn/program/newsupdate/20130911/103458.shtml>

Hughes R, 'A Treaty for Cyberspace' (2010) 86 *International Affairs* 523

Hunker J, Hutchinson R, Margulies J, 'Attribution of Cyber Attacks on Process Control Systems' in Papa M and Shenoi S (eds), *Critical Infrastructure Protection II* (Springer 2008)

Huntley TC, 'Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare' (2010) 60 *Naval Law Review* 1

Hutchins EM, Cloppert MJ and Amin RM, 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains' (paper presented at the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, 17–18 March 2011) <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

ICANN Expert Working Group on gTLD Directory Services, *Initial Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service* (24 June 2013) <https://www.icann.org/en/groups/other/gtld-directory-services/initial-report-24jun13-en.pdf>

Imperva, 'Hacker Intelligence Summary Report – Monitoring Hacker Forums' (October 2011) <http://www.imperva.com/docs/HII_Monitoring_Hacker_Forums.pdf>

Information Warfare Monitor 'Tracking GhostNet: Investigating a Cyber Espionage Network' *Information Warfare Monitor* (1 September 2009) <http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/>

InfoSecurity 'Governments are Big Buyers of Zero-Day Flaws' *InfoSecurity News* (15 July 2013) <http://www.infosecurity-us.com/view/33441/governments-are-big-buyers-of-zeroday-flaws/>

Inkster N, 'China – Threat or Target' (2010) *Montrose Journal* 10

Inter-American Juridical Committee, 'Reaffirmation of Fundamental Principles of International Law' (1942)

International Academy of Astronautics, 'Position Paper on Space Debris Mitigation' (2005) <http://iaaweb.org/iaa/Studies/spacedebrismitigation.pdf>

International Cable Protection Committee, 'About Submarine Telecommunication Cables' (2011) <http://iscpc.org/publications/About_SubTel_Cables_2011.pdf>

International Commission of American Jurists, 'Report Project II, States: Existence, Equality, Recognition' (1927)

International Judical Union, 'Draft of a Declaration of Rights and Duties of Nations' (1919)

Internet Engineering Task Force, 'Internet Protocol, Protocol Specification' (1981) <http://www.ietf.org/rfc/rfc791.txt>

Internet Rights and Privileges Coalition, 'Charter of Human Rights Principles and the Internet' (ver 1.1 Draft 2012) <http://internetrightsandprinciples.org/site/wp-content/uploads/2012/12/Charter-on-Human-Rights-and-Principles-on-the-Internet-Version-1-1-Draft.pdf>

Ipsen K (ed), *Völkerrecht* (6th edn, CH Beck 2010)

Ishac J and Allman M, 'On the Performance of TCP (Transmission Control Protocol) Spoofing in Satellite Networks' (IEEE Milcom, October 2001) <http://icir.org/mallman/papers/milcom01.pdf>

Iwasawa N and Iwatsuki N 'Procedural Conditions' in Crawford J *et al.* (eds), *The Law of International Responsibility* (Oxford University Press 2010)

Japan, Ministry of Defence, 'Toward Stable and Effective Use of Cyberspace' (2012)

Jellenc E, 'Explaining Politico-Strategic Cyber Security: The Feasibility of Applying Arms Race Theory' in Filiol E and Erra R (eds), *11th European Conference on Information Warfare and Security* (Academic Conferences Limited 2012)

Jennings R and Watts A, *Oppenheim's International Law* (9th ed, Oxford University Press 2008)

Jensen ET, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford Journal of International Law* 207

Jentleson B, *Coercive Diplomacy: Scope and Limits in the Contemporary World* (The Stanley Foundation 2006)

Johnson DR and Post D, 'Law And Borders – The Rise of Law in Cyberspace' (1995-1996) 48 *Stanford Law Review* 1367

Johnson N, 'The Disposal of Spacecraft and Launch Vehicle Stages in Low Earth Orbit' (2007) *Proceedings of the Advancement of Space Safety Conference*

Johnstone I, 'The Plea of "Necessity" in International Legal Discourse: Humanitarian Intervention and Counter-Terrorism' (2005) 43 *Columbia Journal of Transnational Law* 337

Jones TY, 'China says willing to discuss cyber security with the U.S.' *Reuters* (12 March 2013) <http://www.reuters.com/article/2013/03/12/us-usa-china-cybersecurity-idUSBRE92A0XO20130312>

Jones, W, 'This Week in Cybercrime: Cybercrime's Industrial Revolution' *IEEE Spectrum* (30 June 2013) <http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-cybercrimes-industrial-revolution>

Joyner CC and Lotrionte C, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 *European Journal of International Law* 825

Jurich JP, 'Cyberwar and Customary International Law: The Potential of a 'Bottom-up' Approach to an International Law of Information Operations' (2008) 9 *Chicago Journal of International Law* 275

Kaiser, SA, 'Automation and Limits of Human Performance: Potential Factors in Aviation Accidents' (2013) *Zeitschrift für Luft- und Weltraumrecht* 207

Kaiser, SA, Satellite Navigation Systems: The Impact of Interoperability (2012) 37 *Annals of Air & Space Law* 369

Kaiser SA, 'UAVs and Their Integration into Non-segregated Airspace' (2011) 36 *Air & Space Law* 161

Kalshoven F, *Belligerent Reprisals* (Martinus Nijhoff 1971)

Kamto, 'The Time Factor in the Application of Countermeasures' in Crawford J, Pellet A and Olleson S (eds), *The Law of International Responsibility* (Oxford University Press 2010)

Kanuck S, 'Sovereign Discourse on Cyber Conflict under International Law' (2009-2010) 88 *Texas Law Review* 1571

Kanwal G, 'China's Emerging Cyber War Doctrine' (2009) 3 *Journal of Defence Studies* 14

Karp, J, 'Mile High Assaults: Air Carrier Liability under the Warsaw Convention' (2000-2001) 66 *Journal of Air Law & Commerce* 1551

Kaspersky Labs, '"Red October" Diplomatic Cyber Attacks Investigation' (Report, 14 January 2013) <http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation>

Kastenberg JE, 'Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law' (2009) 64 *Air Force Law Review* 43

Kaye S, 'International Measures To Protect Oil Platforms, Pipelines, and Submarine Cables from Attack' (2006-2007) 31 *Tulane Maritime Law Journal* 377

Kaye S, 'Submission: Proposed Protection Zones off Sydney' (2006) <http://www.acma.gov.au/webwr/_assets/main/lib100668/professor%20kaye%20(uni%20of%20wollongong).pdf>

Kazazi M, *Burden of Proof and Related Issues - A Study on Evidence before International Tribunals* (Kluwer Law International 1996)

Keber TO and Roguski PN, 'Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis' (2011) 49 *Archiv des Völkerrechts* 399

Keegan J, *Intelligence in War: Knowledge of the Enemy from Napoleon to al-Qaeda* (Hutchinson 2004)

Keller H, 'Friendly Relations Declaration (1970)' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Keller P, 'Cyberpower: Die Strategische Dimension' (2012) *IT-Report*

Kennedy P, *Aufstieg und Fall der großen Mächte* (Fischer 2002)

Keohane RO and Nye JS, *Power and Interdependence: World Politics in Transition* (Little, Brown and Company 1977)

Kerschischnig G, *Cyberthreats and International Law* (Eleven International 2012)

Kesan JP and Hayes CM, 'Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,' (2012) 25 *Harvard Journal of Law & Technology* 482

Khazan O, 'The Creepy, Long-Standing Practice of Undersea Cable Tapping' *The Atlantic* (16 July 2013) <http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>

Kish J, *International Law and Espionage* (Martinus Nijhoff 1995)

Klabbers J, *An Introduction to International Institutional Law* (2nd ed, Cambridge University Press 2009)

Klabbers J, 'Back to Front: Positivism, Constitutionalism, and Accountability', in d'Aspremont J and Kammerhofer J (eds), *International Legal Positivism in a Post-modern World* (Cambridge University Press, forthcoming)

Klabbers J, *International Law* (Cambridge University Press 2013)

Klabbers J, 'Self-control? International Organizations and the Quest for Accountability', in Evans M and Koutrakos P (eds), *The International Responsibility of the European Union: European and International Perspectives* (Hart 2013) 75

Klein E, 'Gegenmaßnahmen' (1997) 37 *Berichte der Deutschen Gesellschaft für Völkerrecht* 39

Klein P, 'The Attribution of Acts to International Organizations', in Crawford J, Pellet A and Olleson S (eds), *The Law of International Responsibility* (Oxford University Press 2010) 297

Klimburg A, 'Mobilising Cyber Power' (2011) 53 *Survival* 41

Klimburg A (ed), *National Cyber Security Framework Manual* (NATO CCD COE Publication 2012)

Klimburg A and Tiirmaa-Klaar H, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU* (European Parliament, Directorate-General for External Policies, Policy Department, SEDE 2011)

Koh HH, *International Law in Cyberspace*, Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland (18 September 2012), *reprinted in* (2012) 54 *Harvard International Law Journal online* 1

Koivoruva T, 'Due Diligence' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Kolb R, 'Principles as Sources of International Law (With Special Reference to Good Faith)' (2006) 53 *Netherlands International Law Review* 1

Korea Herald, '35m Cyworld, Nate users' information hacked' *Korea Herald* (28 July 2011) <http://www.koreaherald.com/view.php?ud=20110728000881>

Koroma AG, 'Solidarity: Evidence of an Emerging International Legal Principle' in Hestermeyer HP, König D, Matz-Lück N, Röben V, Seibert-Fohr A, Stoll PT and Vöneky S (eds), *Coexistence, Cooperation and Solidarity. Liber Amicorum Rüdiger Wolfrum* (vol 1, Martinus Nijhoff 2011)

Koskenniemi M,' Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law' (*Report of the Study Group of the International Law Commission*, UN Doc. A/CN.4/L.682, 13 April 2006)

Koskenniemi M, 'Hierarchy in International Law: A Sketch' (1997) 8 *European Journal of International Law* 566

Koskenniemi M, 'The Politics of International Law' (1990) 1 *European Journal of International Law* 4

Kosugia T, Tokimatsub K, Kurosawab A, Itsuboc N, Yagitad H and Sakagamie M, 'Internalization of the External Costs of Global Environmental Damage in an Integrated Assessment Model' (2009) 37 *Energy Policy* 2664

Kramer FD, Starr SH and Kramer FD (eds), *Cyberpower and National Security* (Potomac Books Inc. 2009)

Krebs B, 'Security Fix - Report: Russian Hacker Forums Fueled Georgia Cyber Attacks' *Washington Post* (16 October 2008) <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html>

Krekel B, Bakos G and Barnett C, 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation' (Northrop Grumman Corporation 2009) <http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved Report_16Oct2009.pdf>

Krieger H, 'Krieg gegen anonymous. Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar' (2012) 50 *Archiv des Völkerrechts* (1) 1

Ku C and Diehl PF (eds), *International Law - Classic and Contemporary Readings* (Lynne Rienner 2009)

Kulesza J, 'State Responsibility for Cyber-Attacks on International Peace and Security' (2009) 29 *Polish Yearbook of International Law* 139

Kulesza J, *International Internet Law* (Routledge 2012)

Kunig P, 'Intervention, Prohibition of' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Kurbalija J, *An Introduction to Internet Governance* (DiploFoundation 2011)

Kurbalija J, 'Do e-mail and e-documents have diplomatic protection?' *Diplo* (Geneva, 13 June 2013) <http://www.diplomacy.edu/blog/do-e-mail-and-e-documents-have-diplomatic-protection>

Kurbalija J, 'How will Wikileaks affect diplomacy?' *Diplo* (Geneva, 1 December 2010) <http://www.diplomacy.edu/blog/how-will-wikileaks-affect-diplomacy>

Kurbalija J, 'Internet Fraud in Diplomacy' (*Reflections on Diplomacy*, 3 December 2011) <http://deepdip.wordpress.com/2011/12/03/internet-fraud-in-diplomacy/>

Kurbalija J, 'Is tweeting a breach of diplomatic function?' *Diplo* (Malta, 2012) <http://www.diplomacy.edu/blog/tweeting-breach-diplomatic-function#_ftn1>

Kurbalija J, 'The Impact of the Internet and ICT on Contemporary Diplomacy' in Kerr P and Wiseman G (eds) *Diplomacy in a Globalizing World Theories and Practices* (Oxford University Press 2012)

Kurbalija J, 'World summit on Information Society and the Development of Internet Diplomacy' in Gatt M and Fsadni AR (eds), *Governing the Internet* (Malta: Academy for the Development of a Democratic Environment, 2011) ch. 2 <http://thinkingeurope.eu/sites/default/files/publication-files/governing_the_internet.pdf>

Kurtz, 'Adjudging the Exceptional at International Investment Law: Security, Public Order and Financial Crisis' (2010) 59 *International & Comparative Law Quarterly* 325

Lachow I, *Active Cyber Defence – A Framework for Policymakers* (Center for a New American Security Policy Brief 2013) <http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf>

Lachowski Z, 'Confidence-Building Measures' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Lachs M, *The Law of Outer Space, An Experience in Contemporary Law-Making* (Slither 1972, *reprinted in* 2010)

Lagoni R, *Legal Aspects of Submarine High Voltage Direct Current (HVDC) Cables* (LIT Verlag 1999)

Lam O, 'South Korea: Internet "Real Name" Violates the Constitution' *Global Voices* (28 August 2012) <http://advocacy.globalvoicesonline.org/2012/08/28/south-korea-internet-real-name-law-violates-the-constitution/>

Landler M and Markoff J, 'In Estonia, what may be the first war in cyberspace' *New York Times* (28 May 2007) <http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html>

Lang W, 'UN-Principles and International Environmental Law' (1999) 3 *Max Planck Yearbook of United Nations Law* 157

Larsson M-L, 'Legal Definitions of the Environment and of Environmental Damage' (1999) 38 *Scandinavian Studies in Law* 155

Lastowka G, 'Paving the Path of Cyberlaw' (2011) 38 *William Mitchell Law Review* 1

Laursen A, 'The Use of Force and (the State of) Necessity' (2004) 37 *Vanderbilt Journal of Transnational Law* 485

Lawrence TJ, *The Principles of International Law* (7th ed, Heath & Co 1910)

Lawton G, 'On the trail of the conficker worm' (2009) 42 *Computer* 19

Leder F, Werner T and Martini P, 'Proactive Botnet Countermeasures – An Offensive Approach' in Czosseck C and Geers K (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009)

Leigh D, 'How 250,000 US embassy cables were leaked' *The Guardian* (28 November 2010) <http://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked>

Lenway SA, 'Between War and Commerce: Economic Sanctions as a Tool of Statecraft' (1988) 42 *International Organization* 397

Lepard BD, *Customary International Law. An New Theory with Practical Implications* (Cambridge University Press 2010)

Lesaffre H, 'Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Countermeasures' in Crawford J *et al.* (ed), *The Law of International Responsibility*, (Oxford University Press 2010) 439

Lessig L, *Code and Other Laws of Cyberspace* (Basic Books 2000)

Lessig L, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501

Levi M, 'Measuring the Cost of Cybercrimes' *ECRIM News Special Edition: Cybercrime and Privacy Issues* (2012) <http://ercim-news.ercim.eu/en90/special/measuring-the-cost-of-cybercrimes>

Lewis J, 'Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia' (Lowy Institute MacArthur Asia Security Project 2013) <http://csis.org/publication/hidden-arena-cyber-competition-and-conflict-indo-pacific-asia>

Lewis JA, 'Confidence-building and international agreement in cybersecurity' in Vignard K (ed), *Confronting Cyberconflict* (UNIDIR Disarmament Forum Series 2011/4)

Lewis JA, 'Conflict and Negotiation in Cyberspace' (Centre for Strategic and International Studies 2013), <https://csis.org/publication/conflict-and-negotiation-cyberspace>

Lewis JA, 'Cybersecurity and Cyberwarfare: Assessment of National Doctrine and Organisation' in UNIDIR, *The Cyber Index. International Security Trends and Realities* (UNIDIR 2013/3)

Lewis JA, 'The Cyber War Has Not Begun' (Center for Strategic and International Studies 2010) <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Cyber+War+Has+Not+Begun#0>

Lewis JA and Timlin K, *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization* (UNIDIR 2011) <http://unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf>

Lewis JE, 'The Economic Espionage Act and the Threat of Chinese Espionage in the United States' (2008-2009) 8 *Chicago-Kent Journal of Intellectual Property* 189

Leyden J, 'Inside the Mysterious US Satellite Hacking Case' *The Register* (21 November 2011) <http://www.theregister.co.uk/2011/11/21/us_sat_hack_mystery/>

Li S, When Does Internet Denial Trigger the Right of Armed Self-Defense? (2013) 38 *Yale Journal of International Law* 179

Lieberman P, 'We're losing the battle against state sponsored attacks' *Help Net Security* (8 April 2013) <http://www.net-security.org/article.php?id=1825>

Lin HS 'Arms Control in Cyberspace: Challenges and Opportunities' *World Politics Review* (6 March 2012) <http://www.worldpoliticsreview.com/articles/print/11683>

Lin HS, 'Offensive Cyber Operations and the Use of Force' (2010) 4 Jo*urnal of National Security Law & Policy* 63

Lindinger M, 'Kampf gegen Weltraumschrott. Wir haben unsere Warnschüsse gehabt' *FAZ* (22 April 2013) <http://www.faz.net/aktuell/gesellschaft/umwelt/kampf-gegen-weltraumschrott-wir-haben-unsere-warnschuesse-gehabt-12158437.html>

Lipson HF, *Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues* (Carnegie Mellon Software Engineering Institute 2002) <http://www.sei.cmu.edu/library/abstracts/reports/02sr009.cfm>

Lobel J, 'The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan' (1999) 24 *Yale Journal of International Law* 537

Lohr S, 'Soviets and Swedes Sparring Over Submarines' *New York Times* (14 January 1988) <http://www.nytimes.com/1988/01/14/world/soviet-and-swedes-sparring-over-submarines.html>

Lowe V, 'Precluding Wrongfulness or Responsibility: A Plea for Excuses' (1999) 10 *European Journal of International Law* 405

LS, 'A digital cold war?' *The Economist* (*Babbage blog*, 14 December 2012) <http://www.economist.com/blogs/babbage/2012/12/internet-regulation>

Lyall F, 'The International Telecommunication Union: A World Communications Commission?' in *Proceedings of the Colloquium on the Law of Outer Space* (IISL 1994)

Lyall F and Larsen PB, *Space Law: A Treatise* (Ashgate 2009)

MacAskill E and Borger J 'New NSA leaks show how the USA is bugging its European allies' *The Guardian* (30 June 2013) <http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies>

MacKinnon R, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic 2012)

Mahiou A, 'Interdependence' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Makarov A, 'Transparency and Confidence-Building Measures: Their Place and Role in Space Security' in UNIDIR, *Security in Space. The Next Generation. Conference Report* (UNIDIR 2008)

Malanczuk P, *Akehurst's Modern Introduction to International Law* (Routledge 1997)

Malecki EJ and Wei H, 'A Wired World: The Evolving Geography of Submarine Cables and the Shift to Asia' (2009) 99 *Annals of the Association of American Geographers* 360

Mandiant, *APT1 Report: Exposing One of China's Cyber Espionage Units* (February 2013) <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>

Manfreda P, 'The Reasons for the Arab Spring' (About.com, 2011) <http://middleeast.about.com/od/humanrightsdemocracy/tp/The-Reasons-For-The-Arab-Spring.htm>

Mankiewicz R, 'The 1970 Hague Convention' (1971) 37 *Journal of Air Law & Commerce* 195, 196

Mansel HP, Pfeiffer T, Kronke H, Kohler C and Hausmann R (eds), *Festschrift für Erik Jayme* (vol 2, Sellier 2004)

Mansfield-Devine S, 'Estonia: what doesn't kill you makes you stronger' (2012) *Network Security* 12

Manyika J, Chui M, Bughin J, Dobbs R, Bisson P and Marrs A, *Disruptive technologies: Advances that will transform life, business, and the global economy* (McKinsey Global Institute Report, 2013) <http://www.mckinsey.com/insights/business_technology/disruptive_technologies>

Marauhn T, 'Die Erhaltung der biologischen Vielfalt und die nachhaltige Nutzung ihrer Bestandteile. Rechtsinstitute der Nachhaltigkeit auf der Grundlage des UN-Übereinkommens über die biologische Vielfalt' in Lange K (ed), *Nachhaltigkeit im Recht: eine Annäherung* (Nomos 2003)

Marion NE, 'The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation' (2010) 4 *International Journal of Cyber Criminology* (1&2) <http://www.cybercrimejournal.com/marion2010ijcc.pdf>

Markoff J, 'In Digital Combat, U.S. Finds No Easy Deterrent' *New York Times* (25 January 2010) <http://www.nytimes.com/2010/01/26/world/26cyber.html>

Markoff J and Kramer AE, 'In Shift, U.S. Talks to Russia on Internet Security' *New York Times* (12 December 2009) <http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0>

Markoff J and Kramer AE, 'U.S. and Russia Differ on a Treaty for Cyberspace' *New York Times* (27 June 2009) <http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all&_r=0>

Markoff J and Shanker T, 'Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk' *New York Times* (New York, 1 August 2009) <http://www.nytimes.com/2009/08/02/us/politics/02cyber.html>

Marsden C, 'ISPs: Content Liability, Control and Neutrality' in Walden I (ed), *Telecommunications Law and Regulation* (Oxford University Press 2012)

Marsden C, *Net Neutrality: Towards a Co-Regulatory Solution* (Bloomsbury 2010)

Marson S, 'A Selective History of Internet Technology and Social Work' (1997) 14 *Computers in Human Services* 35

Marsoof A, 'A Case for *Sui Generis* Treatment of Software Under the WTO Regime' (2012) 20 *International Journal of Law & Information Technology* 291

Matte N, *Space Activities and Emerging International Law* (McGill University1984)

Matz-Lück N, 'Treaties, Conflicts between' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Maurer T, 'Cyber Norm Emergence at the United Nations. An Analysis of the Activities at the UN Regarding Cyber-Security' (Harvard University, John F. Kennedy School of Government, Belfer Center for Science and International Affairs, Discussion Paper No. 2011-11, 2011) <http://belfercenter.ksg.harvard.edu/publication/21445/cyber_norm_emergence_at_the_united_nationsan_analysis_of_the_uns_activities_regarding_cybersecurity.html>

Mazzetti M and Sanger DE, 'Security Leader Says U.S. Would Retaliate Against Cyberattacks' *New York Times* (12 March 2013) <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all&_r=0>

McAskill E, Davies N, Hopkins N, Borger J, Ball J, 'GHCQ interception foreign politicians' communications at G20 summit' *The Guardian* (16 June 2013) <http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits>

McCullagh D, 'FBI turns to broad new wiretap method' *CNET News* (30 September 2007) <http://news.cnet.com/FBI-turns-to-broad-new-wiretap-method/2100-7348_3-6154457.html>

McCullagh D, 'NSA chief downplays cybersecurity power grab reports' *CNET News* (21 April 2009) <http://news.cnet.com/8301-13578_3-10224579-38.html>

McDermott R, *The Kazakhstan-Russia Axis: Shaping CSTO Transformation* (The Foreign Military Studies Office 2012) <http://fmso.leavenworth.army.mil/Collaboration/international/McDermott/CSTO_Transformation-final.pdf>

McDougal MS, Lasswell HD and Reisman WM, 'The Intelligence Function and World Public Order' (1973) 46 *Temple Law Quarterly* (3) 395

McDowell R, 'The U.N. Threat to Internet freedom' *Wall Street Journal* (21 February 2012) <http://online.wsj.com/news/articles/SB10001424052970204792404577229074023195322>

McGavran W, 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 *Tulane Journal of Technic and Intellectual Property* 259

McGregor J, *No Ancient Wisdom, No Followers: The Challenges of Chinese Authoritarian Capitalism* (Prospecta Press 2012)

McLaughlin V, *Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind?* (Bachelor thesis, University of Virginia 2012)

Mejía-Kaiser M, *Informal Regulations and Practices in the Field of Space Debris Mitigation* (2009) 34 *Air & Space Law* 1

Mejía-Kaiser M, *La Órbita Geoestacionaria, Instituto de Geofísica* (UNAM, Comunicaciones Técnicas No. 1, 1987)

Mejía-Kaiser M, 'Taking Garbage Outside: The Geostationary Orbit and Graveyard Orbits' *IISL Proceedings on the Law of Outer Space* 2006

Melnitzky A, 'Defending America against Chinese Cyber Espionage Though the Use of Active Defences' (2012) 20 *Cardozo Journal of International and Comparative Law* 538

Merrills JG, *International Dispute Settlement* (5th edn, Cambridge University Press 2011)

Messerschmidt JE, 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm' 52 *Columumbia Journal of Transnational Law* (forthcoming)

Milanovic M, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press 2011)

Miller JH and Page SE, *Complex Adaptive Systems* (Princeton University Press 2007)

Miller RA, 'Trail Smelter Arbitration', in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Minnick W, 'China Cyberwarfare Evidence Now Undeniable – Mandiant, Intercepts' (*The Official Blog of Defense News International*, 19 February 2013) <http://blogs.defensenews.com/intercepts/2013/02/china-cyberwarfare-evidence-now-undeniable-mandiant/>

MIT_Physics, 'Security Flaw Shows Tor Anonymity Network Dominated by Botnet Command and Control Traffic' (*The Physics arXiv Blog*, MIT Technology Review 2013) <http://m.technologyreview.com/view/519186/security-flaw-shows-tor-anonymity-network-dominated-by-botnet-command-and-control/>

Mohamed A.N, 'The Diplomacy of Micro-States' (2002) *Clingendael Discussion Papers in Diplomacy,* No. 78 <http://www.clingendael.nl/publications/2002/20020100_cli_paper_dip_issue78.pdf>

Moran T, 'Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers' *Peterson Institute Policy Brief* (11 May 2013) <http://www.iie.com/publications/interstitial.cfm?ResearchID=2390>

Moore T, 'Introducing the Economics of Cybersecurity: Principles and Policy Options, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy' (Brown University 2010) <http://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf>

Morgan TC and Schwebach VL, 'Fools Suffer Gladly: The Use of Economic Sanctions in International Crises' (1997) 41 *International Studies Quarterly* 27

Morgenthau HL, *Politics among Nations: The Struggle for Power and Peace* (2nd ed, Alfred Knopf 1955)

Morrison C.A, *Voyage into the Unknown, the Search and Recovery of Cosmos 954* (Abe Books 1982)

Morth TA, 'Considering Our Position. Viewing Information Warfare as Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 *Case Western Reserve Journal of International Law* 567

Mosler H, 'General Principles of Law' in Bernhardt R (ed), *Encyclopaedia of Public International Law* (vol 2, North-Holland 1995) 511

Mshvidobadze K, *Russia's Military Alliance Tackles Cybercrime* (Potomac Institute for Policy Studies 2012) <http://pipscyberissues.wordpress.com>

Mudrinich EM, 'Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem' (2012) 68 *Air Force Law Review* 174

Mueller M, Mathiason J and Klein H, 'The Internet and Global Governance: Principles and Norms for a New Regime' (2007) 13 *Global Governance* 237

Müllerson R, '*Ius ad bellum* Plus Ca Change (de Monde) Plus C´est la M´me Chose (le Droit)?' (2002) 7 *Journal of Conflict and Security Law* 149

Mumford E, 'A socio-technical approach to systems design' (2000) 5 *Requirements Engineering* 125

Muralidhar Reddy, 'Maldives opens "virtual embassy"' *The Hindu* (25 May 2007) <http://www.thehindu.com/todays-paper/tp-international/maldives-opens-virtual-embassy/article1847030.ece>

Murphy M, 'How has the Internet affected diplomatic reporting?' *Diplo* (Malta, 01 July 2013) <http://www.diplomacy.edu/blog/how-has-internet-affected-diplomatic-reporting>

Murray A, 'Of Uses and Abuses of Cyberspace: Coming to Grips with the Present Dangers' in Cassese A (ed), *Realizing Utopia - The Future of International Law* (Oxford University Press 2012)

Murty BS, *The International Law of Diplomacy: The Diplomatic Instrument and World Public Order* (Martinus Nijhoff 1989)

Nakashima E, '15 nations agree to start working together to reduce cyberwarfare threat' *Washington Post* (17 July 2010) <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html>

Nakashima E, 'Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies' *Washington Post* (28 May 2013)

Nakashima E, 'U.S. and Russia sign pact to create communication link on cyber security' *Washington Post* (17 June 2013) <http://articles.washingtonpost.com/2013-06-17/world/40025979_1_cyber-security-pact-homeland-security>

Nakashima E, 'Verizon providing all call records to U.S. under court order' *Washington Post* (6 June 2013) <http://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_story.html>

Nandan SN and Rosenne S (eds), *United Nations Convention on the Law of the Sea 1982: A Commentary* (vol III, Martinus Nijhoff 1995)

Natarajan R, 'Ping Tutorial: 15 effective ping Command Examples' (*The Geek Stuff*, 30 November 2009) <http://urli.st/3ur-The-Geek-Stuff/hU-Ping-Tutorial-15-Effective-Ping-Command-Examples>

National Institute of Standards and Technology, 'Guide for Applying the Risk Management Framework to Federal Information Systems' (2010) <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

National Institute of Standards and Technology, 'Guide to Intrusion Detection and Prevention Systems (IDPS)' (NIST 2007) <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

National Science Foundation, 'A Brief History of NSF and the Internet' (*NSF Factsheet*, 13 August 2003) <http://www.nsf.gov/news/news_summ.jsp?cntn_id=103050>

Nazario J (2009) 'Politically Motivated Denial of Service Attacks' in Czosseck C and Geers K (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press 2009)

Neal D, 'European Parliament votes for PRISM snooping investigation' *The Inquirer* (9 July 2013) <http://www.theinquirer.net/inquirer/news/2280187/european-parliament-votes-for-prism-snooping-investigation>

Nelson LDM, 'Submarine Cables and Pipelines' in Dupuy RJ and Vignes D (eds), *A Handbook on the Law of the Sea* (Martinus Nijhoff 1991)

Netanyahu B (ed), *Terrorism. How the West Can Win* (Farrar, Straus and Giroux 1986)

New Zealand, Transport Accident Investigation Commission New Zealand, *Aviation Occurrence Report 03-00* (2000)

Newsom D, 'The New Diplomatic Agenda: Are Governments Ready?' *International Affairs* (January 1989)

Newsweek, 'The Evil (Cyber) Empire' *Newsweek* (12 December 2009) <http://www.thedailybeast.com/newsweek/2009/12/29/the-evil-cyber-empire.html>

Nicolson H, *The Evolution of Diplomatic Method* (Constable & Co Ltd 1954)

Niyungeko G, *La preuve devant les juridictions internationales* (Bruylant 2005)

Nolte G, 'Article 2(7)' in Simma B *et al.* (eds), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012)

Nolte G, 'Die USA und das Völkerrecht' (2003) 78 *Friedens-Warte* 119

Noortmann M, *Enforcing International Law: From Self-help to Self-contained Regimes* (Ashgate 2005)

Nordquist MH, Wolfrum R, Moore JN and Long R (eds), *Legal Challenges in Maritime Security* (Martinus Nijhoff 2008)

Nowak M, *U.N. Covenant on Civil and Political Rights CCPR Commentary* (NP Engle 1993)

Nuclear Suppliers Group, *Guidelines for Nuclear Transfers* (1978)

Nuclear Suppliers Group, *Guidelines for Transfers of Nuclear-Related Dual-Use Equipment, Materials, Software, and Related Technology* (1992)

Numelin R, *The Beginnings of Diplomacy. A Sociological Study of Intertribal and International Relations* (Oxford University Press 1950)

Nye JS Jr, *The Future of Power in the 21st Century* (Public Affairs 2011)

O'Connell DP, in Shearer IA (ed), *The International Law of the Sea* (vol I, The Clarendon Press 1982)

O'Connell ME, 'Cyber Security without Cyber War' (2012) 17 *Journal of Conflict and Security Law* 187

O'Connell ME, 'Evidence of Terror' (2002) 7 *Journal of Conflict and Security Law* 19

O'Connell ME, 'Rules of Evidence for the Use of Force in International Law's New Era' (2006) 100 *Proceedings of the American Society of International Law* 44

O'Connell RL, *Of Arms and Men: A History of War, Weapons, and Aggression* (Oxford University Press 1989)

O'Hara G, 'Cyber-Espionage: A Growing Threat to the American Economy' (2010-2011) 19 *CommLaw Conspectus* 242

O'Keefe R, 'Proportionality' in Crawford J *et al.* (eds), *The Law of International Responsibility,* (Oxford University Press 2010) 1157

Olson P, *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency* (Little, Brown and Company 2012)

OPSWAT, *Antivirus Market Analysis: December 2012 Software management and security solutions* (OPSWAT 2012) <http://www.opswat.com/about/media/reports/antivirus-december-2012>

Organisation européenne pour la recherche nucléaire (CERN), 'The birth of the web' (*CERN*, undated) <http://home.web.cern.ch/about/birth-web>

Organisation for Economic Co-operation and Development, 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy' (OECD Digital Economy Papers No 211, 2012) <http://dx.doi.org/10.1787/5k8zq92vdgtl-en>

Organisation for Security and Co-operation in Europe, 'OSCE can play important role in cyber security, says Estonian Defence Minister' (4 June 2008) <http://www.osce.org/fsc/49775>

Organization for Security and Co-operation in Europe, Parliamentary Assembly, 'Follow-Up on Recommendations in the OSCE PA's Monaco Declaration' (1st Committee, Interim Report for the 2013 Winter Meeting 2013) <http://www.oscepa.org/component/search/?searchword=Interim%20Report%202013&searchphrase=all>

Ottis R, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective' in Remenyi D (ed), *Proceedings of the 7th European Conference on Information Warfare* (Academic Conferences Limited 2008)

Ottis R 'From Pitchforks to Laptops Volunteers in Cyber Conflicts' in Czosseck C and Podins K (eds), *Conference on Cyber Conflict. Proceedings 2010* (NATO CCD COE Publications 2010)

Owens WA *et al., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Research Council 2009)

Oxman BH, 'Jurisdiction of States' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Paganini P, 'Cyber-espionage: The greatest transfer of wealth in history' *H+ Magazine* (1 March 2013) <http://hplusmagazine.com/2013/03/01/cyber-espionage-the-greatest-transfer-of-wealth-in-history/>

Paganini P, 'Operation Red October: Cyber Espionage campaign against many Governments' *The Hacker News* (14 January 2013) <http://thehackernews.com/2013/01/operation-red-october-cyber-espionage.html#ixzz2jfYuhWh3>

Palchetti P, 'Armed Attack against the Military Force of an International Organization and Use of Force in Self-defence by a Troop-Contributing State: A Tentative Legal Assessment of an Unlikely Scenario' (2010) 7 *International Organizations Law Review* 241

Palmer G and Morgan TC, *A Theory of Foreign Policy* (Princeton University Press 2011)

Palojärvi P, *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict* (Erik Castrén Institute 2009)

Panara C, 'Peaceful Coexistence' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Pant H, 'The BRICS Fallacy' *The Washington Quarterly* (Washington, DC, 1 July 2013) 91

Parkins D, 'Sense Sensibilities and Spying' *The Economist* (6 July 2013) 51

Parsons C, 'Is Iran Now Actually Using Deep Packet Inspection?' (*Christopher Parsons,* 2011) <http://www.christopher-parsons.com/is-iran-now-actually-using-deep-packet-inspection/>

Patrick ET, 'Ex-Aide to Blair Says the British Spied on Annan' *New York Times* (27 February 2004) <http://www.nytimes.com/2004/02/27/world/ex-aide-to-blair-says-the-british-spied-on-annan.html>

Patrick S, 'The Group of Eight Summit: One Pillar of Today's "G-x World," Council on Foreign Relations Blog' (*The Internationalist*, 13 June 2013) <http://blogs.cfr.org/patrick/2013/06/13/the-group-of-eight-summit-one-pillar-of-todays-g-x-world/>

Pelican L, 'Peacetime Cyber-Espionage: A Dangerous But Necessary Game' (2010-2011) 20 *CommLaw Conspectus* 370

Pellerinn C, 'Cyber Operations Give Leaders new Options, Official Says' *American Forces Press Service* (12 April 2012) <http://www.defense.gov/News/NewsArticle.aspx?ID=67918>

Pellet A, 'Art. 38' in Zimmermann A *et al.* (eds), *The Statute of the International Court of Justice. A Commentary* (Oxford University Press 2006)

Penney JW, 'Internet Access Rights: A Brief History and Intellectual Origins' (2011-2012) 38 *William Mitchell Law Review* 10

Perek L, 'Rational Space Management' (2004) 53 *Zeitschrift für Luft- und Weltraumrecht* 575-576

Perlroth N and Sanger D, 'New Computer Attacks Traced to Iran, Officials Say' *New York Times* (25 May 2013) A10

Perlroth N, 'Wall Street Journal Announces that it, Too, Was Hacked by the Chinese' *New York Times* (31 January 2013) <http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html>

Perlroth N, 'Washington Post Joins List of News Media Hacked by the Chinese' *New York Times* (1 February 2013) <http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html>

Perlroth N, Larson J and Shane S, 'N.S.A. foils encryption protection around globe' *International Herald Tribune* (7-8 September 2013) 1

Perry W, 'Information Warfare: An Emerging and Preferred Tool of the People's Republic of China. (2007) *Occasional Papers Series* (28) <http://www.offnews.info/downloads/perry_china_iw.pdf>

Peters A, 'International Dispute Settlement: A Network of Cooperational Duties' (2003) 14 *European Journal of International Law* 1

Petersen N, 'Customary Law Without Custom? Rules, Principles, and the Role of State Practice in International Norm Creation' (2008) 23 *American University International Law Review* 275

Phillips M, 'Lavabit and the Right to Private E-Mail' *New Yorker* (11 October 2013) <http://www.newyorker.com/online/blogs/elements/2013/10/lavabit-and-the-right-to-private-email.html>

Pilkington E, 'Washington Post releases four new slides from NSA's Prism presentation' *The Guardian* (30 June 2013) <http://www.guardian.co.uk/world/2013/jun/30/washington-post-new-slides-prism>

Plohmann D, Gerhards-Padilla E and Leder F, 'Botnets: Detection, Measurement, Disinfection & Defence. Information Security' (ENISA 2011) <http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence>

Poitras L and Gellman B, 'U.S, British intelligence mining data from nine U.S. Internet companies in broad secret program' *Washington Post* (6 June 2013) <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>

Poitras L, Rosenbach M, Schmid F, Stark H and Stock J, 'Angriff aus Amerika' *Der Spiegel* (1 July 2013) 76

Porras P, Saidi H and Vinod Y, *An Analysis of Conficker's Logic and Rendezvous Points* (SRI International 2009) <http://mtc.sri.com/Conficker/>

Potter M, 'The Outer Space Cyberspace Nexus: Satellite Crimes' (1994) 94 *IISL Proceedings* 1

Pras A, Sperotto A, Moura G and Drago I, *Attacks by "Anonymous" WikiLeaks Proponents not Anonymous* (University of Twente 2010) <http://doc.utwente.nl/75331/>

Price J and Forrest J, *Practical Aviation Security: Predicting and Preventing Future Threats* (Elsevier 2009)

Prindle D, 'How to Stay Anonymous Online,' *Digital Trends* (16 May 2013) <http://www.digitaltrends.com/computing/how-to-be-anonymous-online/>

Project Grey Goose, 'Project Grey Goose Phase I Report' (Project Grey Goose 2008) <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>

Radsan J, 'The Unresolved Equation of Espionage and International Law' (2006-2007) 28 *Michigan Journal of International Law* 596

RAND Corporation, 'Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP) prepared for the European Defence Agency unclassified summary' (RAND Corporation, 2013)

Randelzhofer A and Dörr O, 'Article 2(4)' in Simma B *et al.* (eds), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012)

Rao S, 'Countermeasures in International Law. The Contribution of the International Law Commission' in *Studi di diritto internazionale in onore di Gaetano Arangio-Ruiz* (Editoriale Scientifica 2004)

Raustiala K, 'The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law' (2002) 43 *Virginia Journal of International Law* 1

Raymond ES, 1996, *The New Hacker's Dictionary* (3rd ed, MIT Press)

Reidenberg JR, '*Lex informatica*: The formulation of information policy rules through technology' (1998) 76 *Texas Law Review* 553

Reimann M, 'The Yahoo Case and Conflicts of Law in the Cyberage' in Ku C and Diehl PF (eds), *International Law – Classic and Contemporary Readings* (Lynne Rienner 2009)

Reinisch A, 'Sachverständigengutachten zur Frage des Bestehens und der Wirkung des völkerrechtlichen Rechtfertigungsgrundes "Staatsnotstand"' (2008) 68 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 4

Reisman WM, 'Assessing Claims to Revise the Law of War' (2003) 97 *American Journal of International Law* 82

Reporters Without Borders 'China' *Reporters Without Borders* (undated) <http://surveillance.rsf.org/en/china/>

Reuters, 'NSA spied on communications of Brazil and Mexico Presidents' *The Guardian US* (2 September 2013) <http://www.theguardian.com/world/2013/sep/02/nsa-spied-mexico-brazil-presidents>

Reuters, 'United Nations says it will contact U.S. over spying report' *Chicago Tribune News* (2 August 2013) <http://articles.chicagotribune.com/2013-08-26/news/sns-rt-us-usa-security-nsa-un-20130825_1_michelle-nichols-u-n-spokesman-farhan-haq-u-s-intelligence>

Rheingold H, *Virtual Communities: Homesteading on the Electronic Frontier* (Addison Wesley 1993)

Rid T, 'Cyber War Will Not Take Place' (2012) 35 *The Journal of Strategic Studies* 5

Rifkind J, 'Cybercrime in Russia' (Center for Strategic and International Studies, 14 July 2011) <http://csis.org/blog/cybercrime-russia>

Rigaux F, 'The Concept of Fact in Legal Science' in Nerhot P (ed), *Law, Interpretation and Reality* (Springer 1990)

Riley M and Lawrence D, 'Hackers Linked to China's Army Seen from EU to DC' *Bloomberg* (26 July 2012) <http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html>

Rinck G, 'Damage caused by Foreign Aircraft to Third Parties' (1951) 28 *Journal of Air Law & Commerce* 405

Roemer R *et. al*, 'Return-Orientend Programming: Systems, Languages, and Applications' (2012) 15 *ACM Trans. Info. & System Security* <http://cseweb.ucsd.edu/~hovav/papers/rbss12.html>

Romano J-A, 'Combating Terrorism and Weapons of Mass Destruction: Reviving the Doctrine of a State of Necessity' (1999) 87 *Georgetown Law Journal* 1023

Roscini M, 'World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 85

Rosenne S, 'United Nations Treaty Practice' (1954) II *Recueil des Cours* 281

Rosenzweig P, 'The Stuxnet Story and Some Interesting Questions' (*Lawfare* blog, 2 June 2012) <http://www.lawfareblog.com/2012/06/the-stuxnet-story-and-some-interesting-questions/>

Russell A, 'CIA plot led to huge blast in Siberian gas pipeline' *The Telegraph* (Washington, 28 February2004) <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html>

Russell FS, *Information Gathering in Classical Greece* (University of Michigan Press 1999)

Russian Federation, 'Convention on International Information Security (Concept)' (2011)

Russian Federation, 'International Code of Conduct for Information Security (Draft)' (2011)

Russian Federation, Ministry of Defence, 'Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space' (2012)

Ryan Y, 'Anonymous and the Arab uprisings' *Aljazeera* (19 May 2011) <http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html>

Ryan Y, 'Tunisia's bitter cyberwar' *Aljazeera* (6 September 2011) <http://www.aljazeera.com/indepth/features/2011/01/201116141458393 62.html>

Ryngaert C, *Jurisdiction in International Law* (Oxford University Press 2008)

Rytter JE, 'Humanitarian Intervention without the Security Council: From San Francisco to Kosovo – and Beyond' (2001) 70 *Nordic Journal of International Law* 121

Safire W, 'The Farewell Dossier' *New York Times* (2 February 2004) <http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html>

Sandifer DV, *Evidence Before International Tribunals* (rev edn, University Press of Virginia 1988)

Sands P, *Principles of International Environmental Law* (2nd edn, Cambridge University Press 2003)

Sanger D, 'Obama Order Sped Up Wave of Cyber Attacks Against Iran' *New York Times* (1 June 2012) <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0>

Sanger D, Barboza D, Perlroth N, 'Chinese Army Unit Is Seen as Tied to Hacking Against U.S' *New York Times* (19 February 2013) A1

Sanger DE, Barboza D and Perlroth N, 'Chinese Army Unit is Seen as Tied to Hacking Against U.S' *New York Times* (18 February 2013) <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all>

Sanger DE and Markoff J, 'After Google Stand on China, U.S. Treads Lightly' *New York Times* (14 January 2010) <http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology&_r=0>

Sari A, 'UN Peacekeeping Operations and Article 7 ARIO: The Missing Link', (2012) 9 *International Organizations Law Review* 77

Schaap Maj AJ, 'Cyber Warfare Operations: Development and Use under International Law' (2009) 64 *Air Force Law Review* 121

Schachter O, 'The Twilight Existence of Nonbinding International Agreements' (1977) 71 *American Journal of International Law* 296

Schachtman N, 'Darpa Looks to Make Cyberwar Routine With Secret "Plan X"' *Wired* (21 August 2012) <http://www.wired.com/dangerroom/2012/08/plan-x/>

Schachtman N and Singer PW, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive' (Brookings Institution Paper, 2011) <http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx>

Scheinin M, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin' (UN GA Doc. A/HRC/13/37, December 2009)

Schindler D and Hailbronner K, *Die Grenzen des völkerrechtlichen Gewaltverbots* (Müller Juristischer Verlag 1986)

Schmalenbach K, *Die Haftung internationaler Organisationen* (Peter Lang 2004)

Schmitt MN, 'Angriffe im Computernetz und das ius *ad bellum*' (1999*) Neue Zeitschrift für Wehrrecht* 177

Schmitt MN, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885

Schmitt MN, 'Cyber Operations and the *Jus Ad Bellum* Revised' (2011) 56 *Villanova Law Review* 569

Schmitt MN, 'Preemptive Strategies in International Law' (2003) 24 *Michigan Journal of International Law* 513

Schmitt MN, 'The 'Use of Force in Cyberspace: A Reply to Dr Ziolkowski' in Czosseck C, Ottis R and Ziolkowski K (eds), *4th International Conference on Cyber Conflict. Proceedings* (NATO CCD COE Publications 2012)

Schmitt MN, 'The Koh Speech and the Tallinn Manual Juxtaposed' (2012) 54 *Harvard International Law Journal Online* 13 <http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/>

Schmitt MN, 'The Sixteenth Waldemar A. Solf Lecture in International Law' (2003) 176 *Military Law Review* 364

Schmitt MN (gen ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)

Schmitt MN, Harrison Dinniss HA and Wingfield TC, 'Computers and War: The Legal Battlespace' (International Humanitarian Law Research Institute, Background Paper 2004)

Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (US Naval War College 2002)

Schnader W, 'Uniform Aviation Liability Act' (1938) 9 *Journal of Air Law* 664,

Schneier B, 'Anonymity and the Internet' (*Bruce Schneier* blog, 3 February 2010) <http://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html>

Schneier B, 'Cryptanalysis of SHA-1' (*Bruce Schneier* blog, 18 February 2005) <https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html>

Schwartau W, 'Striking Back' *Network World Fusion* (11 January 1999) <http://www.networkworld.com/news/0111vigilante.html>

SciEngines, 'Break DES in less than a single day' (*Sciengines.com*, undated) <http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html>

Scola N, 'Ghonim: "Our revolution is like Wikipedia,"' *TechPresident* (14 February 2011) <http://techpresident.com/blog-entry/ghonim-our-revolution-wikipedia>

Scott Cdr RD, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 *Air Force Law Review* 218

SecDev Group The, 'Tracking GhostNet: Investigating a Cyber Espionage Network' *Infowar Monitor Report* (29 March 2009) <http://de.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>

Sechrist M, *Cyberspace in Deep Water: Protecting Undersea Communication Cables By Creating an International Public-Private Partnership* (Harvard Kennedy School 2010) <http://belfercenter.hks.harvard.edu/files/PAE_final_draft_-_043010.pdf>

Segal A and Waxman MC, 'Why a Cybersecurity Treaty Is a Pipe Dream' (*Council on Foreign Relations*, 27 October 2011) <http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325>

Segura-Serrano A, 'Internet Regulation: A Hard-Law Proposal' (2006) 10 *Jean Monnet Working Paper* 1

Sepura K, 'Economic Espionage: The Front Line of a New World Economic War' (1998-1999) 26 *Syracuse Journal of International Law and Commerce* 127

Seyersted 'Diplomatic Freedom of Communication' Scandinavian Studies in Law (Almqvist & Wiksell International 1970)

Shackelford SJ 'From Nuclear War to Net War: Analogising Cyber Attacks in International Law' (2007) 27 *Berkeley Journal of International Law* 191

Shackelford SJ and Andres RB, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2010-2011) 42 *Georgetown Journal of International Law* 971

Shadowserver Foundation 'Statistics on AV Products' (*Shadowserver.org*, 2013) <https://www.shadowserver.org/wiki/pmwiki.php/AV/ImprovementBetweenInitialAndRetests>

Shaffer G and Trachtman J, 'Interpretation and Institutional Choice at the WTO' (2011) 52 *Virginia Journal of International Law* 103

Shakarian P, Shakarian J and Ruef A, 'The Dragon and the Computer: Why Intellectual Property Theft is Compatible with Chinese Cyber-Warfare Doctrine' in Shakarian P, Shakarian J and Ruef A (eds), *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Syngres 2013)

Sharp WG Sr, *Cyberspace and the Use of Force* (Aegis Research Corporation 1999)

Shaw MN, *International Law* (6th edn, Cambridge University Press 2008)

Sheldon JB, 'Achieving Mutual Comprehension: Why Cyberpower Matters to Both Developed and Developing Countries' in Vignard K (ed), *Confronting Cyberconflict* (UNIDIR Disarmament Forum Series 2011/4)

Shelton D, Equity, in Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Sherman L, '"Wildly Enthusiastic" about the First Multilateral Agreement on Trade in Telecommunications Services' (1999) 51 *Federal Communications Law Journal* 61

Shubber S, 'Aircraft Hijacking under the Hague Convention 1970 – A New Regime?' (1973) 22 *International and Comparative Law Quarterly* 687

Siciliano R, 'Seven Types of Hacker Motivations' (*Infosec Island* blog, 25 March 2011) <http://www.infosecisland.com/blogview/12659-Seven-Types-of-Hacker-Motivations.html>

Sicilianos L-A, 'Countermeasures in Response to Grave Violations of Obligations Owed to the International Community', in Crawford J *et al.* (eds) *The Law of International Responsibility* (Oxford University Press 2010)

Sick G, 'The Carter Administration' in Wright R (ed), *The Iran Primer: Book Overview* (United States Institute for Peace 2010) <http://iranprimer.usip.org/resource/carter-administration-0>

Silver DB, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' in Schmitt NM and O'Donnell BT (eds), *Computer Network Attack and International Law* (US Naval War College 2002)

Simma B, 'Counter-measures and Dispute Settlement: A Plea for a Different Balance' (1994) 5 *European Journal of International Law* 102

Simma B, 'From Bilateralism to Community Interest in International Law' (1994) VI *Recueil des Cours* 221

Simma B, 'NATO, the UN, and the Use of Force: Legal Aspects' (1999) 10 *European Journal of International Law* 1

Simma B, Khan D-E, Nolte G and Paulus A (eds), *The Charter of the United Nations. A Commentary* (3rd edn, vol 1, Oxford University Press 2012)

Singel R, 'White House Cyber Czar: "There is No Cyberwar"' *Wired* (4 March 2010) <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>

Singer D, 'In Cyberspace, New Cold War' *New York Times* (24 February 2013) <http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html?pagewanted=all>

Singh N, *Termination of Membership of International Organisations* (Stevens and Sons 1958)

Sklerov Lt MJ, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent' (2009) 201 *Military Law Review* 1

Sloane R, 'On the Use and Abuse of Necessity in the Law of State Responsibility' (2012) 106 *American Journal of International Law* 447

Smale A, 'Anger Growing Among Allies on U.S. Spying' *New York Times* (23 October 2013), <http://www.nytimes.com/2013/10/24/world/europe/united-states-disputes-reports-of-wiretapping-in-Europe.html?_r=0>

Smith JH, 'Keynote Address' (2007) 28 *Michigan Journal of International Law* 544

Smith LJ and Kerrest A, 'Article I, Liability Convention' in Hobe S, Schmidt-Tedd B and Schrogl K-U (eds), *Cologne Commentary on Space Law* (vol 2, Carl Heymanns Verlag 2013) 111

Soares M, 'The Great Brazilian Sat-Hack Crackdown' *Wired* (20 April 2009) <http://www.wired.com/politics/security/news/2009/04/fleetcom?currentPage=all#>

Sofaer AD, 'On the Necessity of Pre-emption' (2003) 15 *European Journal of International Law* 209

Soldatov A and Borogan I, 'The Kremlin's New Internet Surveillance Plan Goes Live Today,' *Wired* (November 2012) <http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/>

Space News, 'Virginia Man Sentenced for Satellite Interference' *Space News* (17 – 23 December 1990)

Spector PL, 'The World Trade Organisation Agreement on Telecommunications' (1998) 32 *The International Lawyer* 217

St John McDonald R, 'Solidarity in the Practice and Discourse of Public International Law' (1996) 8 *Pace International Law Review* 259

Stalinsky S 'China Isn't The Only Source Of Cyberattacks' *Wall Street Journal* (22 May 2013) 17

Standage T, *The Victorian Internet* (Phoenix 1998)

Starr SH, Kuehl D and Pudas T, 'Perspectives on Building a Cyber Force Structure' in Czosseck C and Podins K (eds), *Conference on Cyber Conflict. Proceedings 2010* (NATO CCD COE Publications 2010)

Stein T and Marauhn T, 'Völkerrechtliche Aspekte von Informationsoperationen' (2000) 60 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 1

Sterner E, 'Retaliatory Deterrence in Cyberspace' (2011) 5 *Strategic Studies Quarterly* 62

Stolker C and Levine D, 'Compensation for Damage to Parties on the Ground as a Result of Aviation Accidents' (1997) XXII *Air & Space Law* (2)

Streltsov A, 'International Information Security: Description and Legal Aspects' in Vignard K (ed), *ICTs and International Security* (UNIDIR Disarmament Forum Series 2007/3)

Sulmasy G and Yoo J, 'Counterintuitive: Intelligence Operations and International Law' (2007) 28 *Michigan Journal of International Law* 628

Summerton J, *Changing Large Technical Systems* (Westview Press 1994)

Sydow C, 'NSA-Abhörskandal: Die Datenräuber von der USS "Jimmy Carter"' *Spiegel Online* (1 July 2013) <http://www.spiegel.de/politik/ausland/die-uss-jimmy-carter-soll-fuer-die-nsa-glasfaserkabel-anzapfen-a-908815.html>

Symantec, 'Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually' (*Symantec.com* 2011) <http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02>

Tadjdeh Y, 'U.S. Engaged in "Cyber Cold War" with China, Iran' *National Defence Magazine* (7 March 2013) <http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1075>

Tainter JA, 'Social Complexity and Sustainability' (2006) 3 *Ecological Complexity* 91

Takei Y, 'Law and Policy for International Submarine Cables in the Asia-Pacific Region' (Asian Society of International Law, Working Paper 2010/13) <http://asiansil.org/publications/2010-13%20-%20Yoshinobu%20Takei.pdf>

Tammes JP, 'The Legal System as a Source of International Law' (1953) 1 *Netherlands International Law Review* 374

Tams CJ, 'Light Treatment of a Complex Problem: The Law of Self-Defence in the Wall Case' (2005) *16 European Journal of International Law* 963

Tams CJ, 'The Use of Force Against Terrorists' (2009) 20 *European Journal of International Law* 359

Taylor A, 'Sorry, But That "Chinese" Hacking Report Proves Nothing' *Business Insider* (19 February 2013) <http://www.businessinsider.com/mandiant-china-report-questioned-2013-2>

Teledyne Brown Engineering, 'The Fragmentation of Kosmos 2163' (study prepared for NASA Lyndon B. Johnson Space Center, January 1992) <http://archive.org/stream/nasa_techdoc_19940012030/19940012030_djvu.txt>

Terdiman D, 'Stuxnet delivered to Iranian nuclear plant on thumb drive' *CNET News* (12 April 2012) <http://news.cnet.com/8301-13772_3-57413329-52/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/>

Terekhov AD, 'International Liability for Damage Caused by Space Objects with Nuclear Power Sources on Board' in *Proceedings of the Colloquium on the Law of Outer Space* (IISL 1993)

Terry JP, 'Responding to Attacks on Critical Computer Infrastructure. What Targets? What Rules of Engagement?' in Schmitt NM and O'Donnell BT (eds), *Computer Network Attack and International Law* (US Naval War College 2002)

The American Institute of International Law, 'Declaration of Rights and Duties of Nations' (1916)

The American Law Institute, 'Restatement (Third) of the Foreign Relations Law of the United States (The American Law Institute 1987)

The Internet Engineering Task Force, 'Internet Security Glossary' (vers 2, 2007) <http://tools.ietf.org/html/rfc4949>

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (UN Doc. E/CN.4/1996/39, November 1996)

The Netherlands, Ministry of Defence, *The Cyber Defence Strategy* (2012)

Tiirmaa-Klaar H, Gassen J, Gerhards-Padilla E and Martini P, *Botnets - Springer Briefs in Cybersecurity* (Springer 2013)

Tikk E, 'Global Cybersecurity-Thinking About the Niche for NATO' (2010) 30 *SAIS Review* 105

Tikk E, Kaska K and Vihul L, *International Cyber Incidents: Legal Considerations* (NATO CCD COE Publications 2010)

Tilly C, *Coercion, Capital, and European States, Ad 990-1992* (Blackwell 1992)

Tomuschat C, 'Article 2(3)' in Simma B *et al.* (eds), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012)

Tomuschat C, 'Iraq – Demise of International Law?' (2003) 78 *Friedens-Warte* 141

Touré H, 'The International Response to Cyberwar' in Touré H (ed), *The Quest for Cyberpeace* (ITU and World Federation of Scientists 2011)

Treves T, 'Customary International Law' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Trouwborst A, *Precautionary Rights and Duties of States* (Brill 2006)

Tsagourias N, 'Necessity and the Use of Force: A Special Regime' (2010) 41 *Netherlands Yearbook of International Law* 11

Tsukayama H and Farhi P, 'Syrian hackers claim responsibility for disrupting Twitter' *Washington Post* (27 August 2013) <http://articles.washingtonpost.com/2013-08-27/lifestyle/41497149_1_syrian-electronic-army-amazon-web-services-web-site>

Turilli M, Vaccaro A and Taddeo M, 'The Case of On-line Trust' (2010) 23 *Knowledge Technology and Policy Journal* 333

Ulfstein G, 'Treaty Bodies' in Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Unger N, *Anonymity on the Internet* (University of Virginia 20123) <http://www.cs.virginia.edu/crab/anonymity.ppt>

Union of Soviet Socialist Republics, 'Draft Resolution (Concerning Alleged Aggressive Acts by the United States Air Force Against the Soviet Union)' (UNSC Doc S/4321, 23 May 1960) (not adopted)

United Kingdom, Air Accidents Investigation Branch (AAIB), 'Aircraft Accident Report No 2/90 (EW/C1094). Report on the accident to Boeing 747-121, N739PA at Lockerbie, Dumfriesshire, Scotland on 21 December 1988' (Doc. AAIB AAR 2/90 of 6 August 1990)

United Kingdom, Cabinet Office and Detica Ltd, 'The Cost of Cyber Crime' (17 February 2011) <http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime>

United Kingdom, Centre for the Protection of National Infrastructure (CPNI), 'Cyber Security in Civil Aviation' (CPNI August 2012)

United Kingdom, *The UK Cyber Security Strategy* (November 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>

United Nations Commission on Sustainable Development, 'Report of the Expert Group Meeting on Identification of Principles of International Law for Sustainable Development' (Geneva, Switzerland, 26-28 September 1995)

United Nations Counter-Terrorism Implementation Task Force, 'Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects', CTITF Working Group Compendium (CTITF Publication Series United Nations 2011)

United Nations General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (A/RES/65/201, 2010)

United Nations General Assembly, 'Report of the Committee on the Peaceful Uses of Outer Space' (A/RES/62/20, 2007)

United Nations General Assembly, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (A/RES/68/98, 2013)

United Nations General Assembly, 'Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (A/RES/65/94, 2010)

United Nations General Assembly, 'Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament' (UN Doc A/S-15/3, 1988, endorsed by UNGA A/RES/43/78H, 1988)

United Nations Institute for Disarmament Research, 'The Cyber Index - International Security Trends and Realities' (UNIDIR 2013) <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>

United Nations Materials on the Responsibility of States for Internationally Wrongful Acts (UN Doc. ST/LEG/SER B/25, 2012)

United Nations Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the Context of International Security' (Disarmament Study Series 2011/33) <http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf>

United Nations Office for Outer Space Affairs, 'Current and planned global and regional navigation satellite systems and satellite-based augmentation systems of the International Committee on Global Navigation Satellite Systems Providers' (Forum, New York, 2010, ST/SPACE/50)

United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (February 2013) <http://www.unodc.org/documents/commissions/CCPCJ_session22/13-80699_Ebook_2013_study_CRP5.pdf>

United Nations, Report of the UN Conference on the Human Environment, Stockholm (UN Doc A/CONF48/14/Rev1)

United Nations, Report of the UN Conference on the Human Environment, Stockholm (UN Doc A/CONF48/14/Rev1)

United Nations, Report of the United Nations Conference on Environment and Development (UN Doc A/CONF.151/26/Rev.1 (vol I), 3–14 June 1992)

United States of America Department of Transportation, *Federal Radionavigation Plan 2012*

United States of America State Department, 'Major Programs of IRM's Office of eDiplomacy' (U.S. Department of State 2013) <http://www.state.gov/m/irm/ediplomacy/c23840.htm>

United States of America, Chamber of Commerce, 'US Chamber of Commerce Annual Report to Congress' (2012) <http://www.uscc.gov/annual_report/2012/2012-Report-to-Congress.pdf>

United States of America, Department of Defense, 'Cyberspace Policy Report' (Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011) (USDoD, 2011)

United States of America, Department of Defense, 'Defense Department Cyber Efforts: Definitions, Focal Point and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates' (US Department of Defense, Memo CM-0477-08, 2011) <http://www.gao.gov/assets/100/97675.html>

United States of America, Department of Defense, Defense Science Board, 'Task Force Report: Resilient Military Systems and the Advanced Cyber Threat' (2012)

United States of America, Department of Defense, Office of Legal Counsel, 'An Assessment of International Legal Issues in Information Operations' (May 1999) <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>

United States of America, Department of Defense, *Strategy for Operating in Cyberspace* (2011) <http://www.defense.gov/news/d20110714cyber.pdf>

United States of America, Department of Defense, *The Strategy for Homeland Defence and Civil Support* (USDoD 2005)

United States of America, Department of State, *Diplomatic Aircraft Clearance Procedures for Foreign State Aircraft to Operate in The United States National Airspace* (undated) <http://www.state.gov/t/pm/iso/c56895.htm>

United States of America, Department of Transportation, Federal Aviation Administration, PED Aviation Rulemaking Committee (ARC), 'FAA to Allow Airlines to Expand Use of Personal Electronics' (Press Release 31 October 2013) <http://www.faa.gov/news/press_releases/news_story.cfm?newsId=15254>

United States of America, Federal Aviation Administration, 'A Report from the Portable Electronic Device Aviation Rule Making Committee to the Federal Aviation Administration' (30 September 2013) <http://www.faa.gov/about/initiatives/ped/media/ped_arc_final_report.pdf>

United States of America, Government Accountability Office, 'Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance' (GAO-10-606, 2 July 2010) <http://www.gao.gov/products/GAO-10-606>

United States of America, Mission to the OSCE, 'Informal Working Group Established by PC Decision 1039: Revised Draft Set of CBMs' (Doc No PC.DEL/871/Rev.1, 2012) <http://www.paranoia.net/assessment/at/OSCE_Reprise/pcdel0871r1%20usa%2c%20draft%20set%20cbms.pdf>

United States of America, National Security Agency, 'Encrypting Files with WinZip®' (2007) <http://www.nsa.gov/ia/_files/factsheets/I735-002-08.pdf>

United States of America, Office of the National Counterintelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace' (Report to the Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011)

United States of America, Office of the National Counterintelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace' (October 2011) <http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf>

United States of America, Office of the President of the United States, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (February 2013) <http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>

United States of America, Office of the President of the United States of America, Presidential Policy Directive/PPD-20 (TOP SECRET/NOFOR), U.S. Cyber Operations Policy (available on WikiLeaks)

United States of America, Office of the President of the United States, 'Annual Report of the President of the United States on the Trade Agreements Program' (1999) <http://www.ustr.gov/sites/default/files/AnnualReport%20Final2013.pdf>

United States of America, Office of the President of the United States, *International Strategy for Cyberspace, Prosperity, Security and Openness in a Networked World* (May 2011)

United States of America, Office of the Secretary of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013' (2013) <http://www.defense.gov/pubs/2013_china_report_final.pdf>

United States of America, State Department, 'IT Strategic Plan: Fiscal Years 2011-2013 – Digital Diplomacy'

United States of America, State Department, 'U.S. Model BIT' (2012) <http://www.state.gov/e/eb/ifd/bit/index.htm>

United States of America, The President's National Security Telecommunications Advisory Committee (NSTAC), 'Report to the President on International Communications' (NSTAC 2007)

United States of America, U.S. Navy/U.S. Marine Corps/U.S. Coast Guard, *The Commander's Handbook on the Law of Naval Operations* (NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, 2007)

United States of America, U.S.-China Economic and Security Review Commission, 'Annual Report to Congress of the U.S.-China Economic and Security Commission' (112th Congress, 2nd Session, November 2012) <http://www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf >

United States of America, United States Air Force, 'Air Force Basic Doctrine Document 1' (17 November 2003)

Utton AE, 'Protective Measures and the *Torrey Canyon*' (1968) 9 *Boston College Industrial and Commercial Law Review* 613

Vaarandi R, *Cyber Defense Monitoring Solutions Course: Event logs and syslog* (NATO Cooperative Cyber Defence Centre of Excellence 2013)

Valeriano B, 'Mind the Gap? Deterrence in Cyberspace' *New Atlanticist* (11 July 2012) <http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace>

Van Dinh T, *Communication and Diplomacy in a Changing World* (Ablex 1987)

Vatis M, 'The Council of Europe Convention on Cybercrime' in *Proceedings of the National Research Council Workshop on Deterring Cyber Attacks* (The National Academic Press 2010)

Vatutin A,'Russia seeks equal cybersecurity for all' *The Voice of Russia* (23 September 2011) <http://english.ruvr.ru/2011/09/23/56634644.html>

Venzke I and von Bernstorff J, 'Ethos, Ethics, and Morality in International Relations' in: Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Verdirame G, *The UN and Human Rights: Who Guards the Guardians?* (Cambridge University Press 2011)

Vernet P.M, 'Pulp Mills on the River Uruguay (Argentina v Uruguay)' in Wolfrum R (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Verwey D, *The European Community, the European Union and the International Law of Treaties* (T.M.C. Asser Press, 2004)

Vignard K (ed), *Confronting Cyberconflict* (UNIDIR Disarmament Forum Series 2011/4 2012)

Viñuales JE, 'Legal Techniques for Dealing with Scientific Uncertainty in Environmental Law', (2010) 43 *Vanderbilt Journal of Transnational Law* 437

Vitzthum Graf W (ed), *Völkerrecht* (De Gruyter 2001)

von Bogdandy A, 'General Principles of International Public Authority: Sketching a Research Field' (2008) 9 *German Law Journal* 1909

von Bogdandy A *et al.* (eds), *The Exercise of Public Authority by International Institutions: Advancing International Institutional Law* (Springer 2010)

Vöneky S, 'Analogy in International Law' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Voß O, 'Überwachungs-Software: Auf der Spur des Trojaners' *Wirtschaftswoche* (10 October 2011) <http://www.wiwo.de/technologie/digitale-welt/ueberwachungs-software-auf-der-spur-des-trojaners/5756462.html>

Wagner E, 'Submarine Cables and Protections Provided by the Law of the Sea' (1995) 19 *Marine Policy* 127

Waibel M, 'Two Worlds of Necessity in ICSID Arbitration: CMS and LG&E' (2007) 20 *Leiden Journal of International Law* 637

Walker B and Salt D, *Resilience Thinking: Sustaining Ecosystems and People in a Changing World* (Island Press 2006)

Walker G (ed), *Definitions for the Law of the Sea* (Martinus Nijhoff 2012)

Wall Street Journal, 'Twitter Helps in Haiti Quake Coverage, Aid' *Wall Street Journal* (14 January 2010) <http://blogs.wsj.com/digits/2010/01/14/twitter-helps-in-haiti-quake-coverage-aid/>

Waltz KN, *Theory of International Politics* (McGraw-Hill 1979)

Waxman MC, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 *Yale Journal of International Law* 421

Waxman MC, 'Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions' (2013) 89 *International Law Studies* 109

Wedgwood R, 'Responding to Terrorism: The Strikes Against bin Laden' (1999) 24 *Yale Journal of International Law* 559

Weigand, T, 'Accident, Exclusivity and Passenger Disturbances under the Warsaw Convention' (2001) 16 *American University International Law Review* 890

Weiner N, *Cybernetics or Control and Communication in the Animal and the Machine* (MIT Press 1965)

Wendel P, *State Responsibility for Interferences with the Freedom of Navigation in Public International Law* (Springer 2007)

West Z, 'Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback' (2012) 63 *Syracuse Law Review* 119

Westlake A, 'Japan pushes to form cyber-defense network with other ASEAN countries' *Japan Daily Press* (8 October 2012) <http://japandailypress.com/japan-pushes-to-form-cyber-defense-network-with-other-asean-countries-0814818/>

Wheeler DA and Larsen GN, *Techniques for Cyber Attack Attribution* (Institute for Defense Analysis 2003) <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859>

Whiteman, H, 'Cyber Terrorism and Civil Aviation' in Sofaer AD and Goodman SE (eds), *Transnational Dimension of Cyber Crime and Terrorism* (Hoover Press 2001) 73

Whitman M and Mattord V, *Principles of Information Security* (Delmar 2008)

Whitney L, 'China blames U.S. for most cyberattacks against military Web sites' *CNET News* (28 February 2013) <http://news.cnet.com/8301-1009_3-57571811-83/china-blames-u.s-for-most-cyberattacks-against-military-web-sites>

Whitney L, 'North Korea Behind March Cyber Attack, says South Korea' *CNET News* (10 April 2013) <http://news.cnet.com/8301-1009_3-57578829-83/north-korea-behind-march-cyberattack-says-south-korea/>

Wiener JB, 'Precaution' in Bodansky D, Brunnée J and Hey E (eds), *The Oxford Handbook of International Environmental Law* (Oxford University Press 2007)

Williams F, 'Radio spectrum freed for mobiles' *Financial Times* (19 November 2007)

Williams P, 'The African Union's Conflict Management Capabilities' (*IIGG Working Paper* 2011) <http://www.cfr.org/regional-security/african-unions-conflict-management-capabilities/p26044?cid=ppc-Google-african_union_paper&gclid=CJaguJityLkCFQMd3godeVoAHg>

Williams RD, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2010-2011) 79 *George Washington Law Review* 1164

Wines M, 'French Said to Spy on U.S. Computer Companies' *New York Times* (18 November 1990) <http://www.nytimes.com/1990/11/18/world/french-said-to-spy-on-us-computer-companies.html>

Winter M, 'NSA uses supercomputers to crack Web encryption, files show' *USA Today* (5 September 2013) <http://www.usatoday.com/story/news/nation/2013/09/05/nsa-snowden-encryption-cracked/2772721/>

WIPO, Summary of the WIPO Copyright Treaty (WCT) <http://www.wipo.int/treaties/en/ip/wct/summary_wct.html>

Wired Magazine, 'Facebook, Twitter Help the Arab Spring Blossom' *Wired Magazine* (16 April 2013), <http://www.wired.com/magazine/2013/04/arabspring/>

Witten S, 'Introductory note to the Convention on Suppression of Unlawful Acts relating to International Civil Aviation and the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft' (2011) 50 *International Legal Materials* 141

Wolfrum R, 'Article 1' in Simma B *et al.* (eds), *The Charter of the United Nations* (3rd edn, vol 1, Oxford University Press 2012)

Wolfrum R, 'Common Heritage of Mankind' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Wolfrum R, 'Co-operation, International Law of' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Wolfrum R, 'General International Law (Principles, Rules, and Standards)' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Wolfrum R, 'International Courts and Tribunals, Evidence' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Wolfrum R, 'Sources of International Law' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Wolfrum R, 'The Attack of September 11, 2001, the Wars Against the Taliban and Iraq: Is There a Need to Reconsider International Law on the Recourse to Force and the Rules in Armed Conflict?' (2003) 7 *Max Planck Yearbook of United Nations Law* 1

Wolfrum R (ed), *The Max Planck Encyclopaedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Wolfrum R and Philipp C (eds), *United Nations: Law, Policies and Practice* (vol I, CH Beck 1995)

Woltag J-C, 'Cyber Warfare' in Wolfrum R (ed), *Max Planck Encyclopaedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Woltag J-C, 'Internet' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

World Health Organization, 'The Right to Water' (Geneva, 2003) <http://www2.ohchr.org/english/issues/water/docs/Right_to_Water.pdf>

Wortham A, 'Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?' (2011-2012) 64 *Federal Communications Law Journal* 643

Wrathall LR, 'The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward' (2010-2011) 12 *San Diego International Law Journal* 223

Wright Q, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' in Stanger RJ (ed), *Essays on Espionage and International Law* (Ohio State University Press 1962)

Wright Q, 'The Role of International Law in Contemporary Diplomacy' in SD Kertesz and Fitzsimons MA (eds), *Diplomacy in a Changing World* (University of Notre Dame 1959)

Wu CC, Chen KT, Chang YC and Lei CL, *Detecting VoIP Traffic Based on Human Conversation Patterns* (SINICA 2013) <http://www.iis.sinica.edu.tw/~swc/pub/voip_traffic_detection.html>

Yannaca-Small K, 'Essential Security Interests under International Investment Law' (chapter 5) in OECD, *International Investment Perspectives: Freedom of Investment in a Changing World* 93-134 (OECD 2007)

Yee S, 'The Potential Impact of the Possible US Responses to the 9-11 Atrocities on the Law regarding the Use of Force and Self-Defence' (2002) 1 *Chinese Journal of International Law* 287

Young IM, *Responsibility for Justice* (Oxford University Press 2011)

Zakaria F, *The Post-American World* (WW Norton 2008)

Zemanek K, 'Armed Attack' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) <www.mpepil.com>

Ziegler K, 'Domaine Réservé' in Wolfrum R (ed), *The Max Planck Encyclopedia of Public International Law* (Oxford University Press, online edition) < www.mpepil.com>

Zimmermann A, Oellers-Frahm K and Tomuschat C (eds), *The Statute of the International Court of Justice. A Commentary* (Oxford University Press 2006)

Zimmermann A, The Second Lebanon War: *Jus ad Bellum, Jus in Bello* and the Issue of Proportionality, (2007) 11 *Max Planck Yearbook of United Nations Law* 99

Ziolkowski K, 'Computer Network Operations and the Law of Armed Conflict' (2010) 49 *Military Law and the Law of War Review* 47

Ziolkowski K, *Confidence Building Measures for Cyberspace – Legal Implications* (NATO CCD COE Publication 2013)

Ziolkowski K, *Gerechtigkeitspostulate als Rechtfertigung von Kriegen. Zum Einfluss moderner Konzepte des Gerechten Krieges auf die völkerrechtliche Zulässigkeit zwischenstaatlicher Gewaltanwendung nach 1945* (NOMOS 2008)

Ziolkowski K, '*Ius ad Bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force', in Czosseck C, Ottis R and Ziolkowski K (eds), *2012 4th International Conference on Cyber Conflict* (Tallinn, NATO CCD COE Publications 2012) 295

Ziolkowski K, 'Stuxnet- Legal Considerations' (2012) 25 *Humanitäres Völkerrecht □ Informationsschriften / Journal of International Law of Peace and Armed Conflict* 139

Zittrain JL, 'The Generative Internet' (2006) 119 *Harvard Law Review* 1974

Zoller E, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational Publishers 1984)

Zutshi B, 'GATS: Impact on developing countries and telecom services' (1994) July–August *Transnational Data and Communications Report* 24

Cases and Advisory Opinions

A. Ahlstrom Oy v Commission, Joined Cases 89, 104, 114, 116, 117 and 125 to 129/85, (1988) ECR 05193

Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, (2010) ICJ Rep 403

Affaire des biens britanniques au Maroc espagnol (Espagne v Royaume-Uni), (1925) 2 R.I.A.A. 615

Agent Judiciaire de Trésor Public v *Caisse Primaire de Sécurité Sociale de la Charente-Maritime et Range*, Poitiers Court of Appel, 24 October 1961, 49 ILR 500

Air France v Saks, 470 US 392 (S. Ct. 1985) 399

Air Services Agreement Arbitral Award (United States of America v France), (1978) 18 R.I.A.A. 417

Appeal Relating to the Jurisdiction of the ICAO Council (India v Pakistan), (1972) ICJ Rep 46

Applicability of the Obligation to Arbitrate under Section 21 of the United Nations Headquarters Agreement of 26 June 1947, Advisory Opinion, (1988) ICJ Rep 12

Application of the Interim Accord of 13 September 1995 (The Former Yugoslav Republic of Macedonia v Greece), (2011) ICJ Rep 644

Archer Daniels Midland Company v. Mexico, Award, ICSID (2007) Case No. ARB(AF)/04/05

Arrest Warrant Case (Democratic Republic of Congo v Belgium), (2002) ICJ Rep 3

Article 3, Paragraph 2, of Treaty of Lausanne, Advisory Opinion, (1925) PCIJ Rep Series B No 12

B.B. v. France, ECtHR 47/1998/950/1165

Bankovic and others v *Belgium and others*, (1999) ECtHR 52207/99

Behrami and Behrami v *France* and *Saramati* v *France and others*, (2001) ECtHR 71421/01

Belgium – Measure affecting commercial telephone directory services, 13 May 1997, WTO WT/DS80

Boyd v White, 128 Cal. App. 2d 641

Branno v *Ministry of War*, 14 June 1954, 22 ILR 756

Brazil – Measures Affecting Imports of Retreaded Tyres, (2007) WTO WT/DS332/AB/R

Caisse Primaire et Caisse Régionale de Sécurité Sociale de Thionville v *Agent Judiciare de Trésor*, (1961) 49 ILR 498

Case C-7/97 Oscar Bronner GmbH & Co KG v Mediaprint Zeitungs-und Zeitschriftenverlag GmbH & Co KG and Others, (1998) ECR I-7791

Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), (2007) ICJ Rep 43

Case concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda), (2005) ICJ Rep 116

Case concerning Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada v United States of America), (1984) ICJ Rep 246

Case concerning Land and Maritime Boundary Between Cameroon and Nigeria Case (Cameroon v Nigeria), Preliminary Objections, (1998) ICJ Rep 275

Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States), Merits, (1986) ICJ Rep 14

Case concerning Pulp Mills on the River Uruguay (Argentine v Uruguay), (2010) ICJ Rep 14

Case concerning Right of Passage over Indian Territory Case (Portugal v India), Preliminary Objections, (1957) ICJ Rep 125

Case concerning Territorial and Maritime Dispute between Nicaragua and Honduras in the Caribbean Sea (Nicaragua v Honduras), (2007) ICJ Rep 659

Case concerning the Barcelona Traction, Light and Power Company Limited (Belgium v Spain), (1970) ICJ Rep 3

Case concerning the Difference Between New Zealand and France Concerning the Interpretation or Application of two Agreements, Concluded on 9 July 1986 Between the two States and Which Related to the Problems Arising from the Rainbow Warrior Affair (New Zealand v. France), (1990) 20 R.I.A.A. 217

Case concerning the Factory at Chorzów (Germany v Poland), Merits, (1928) PCIJ Rep Series A No 17

Case concerning the Frontier Dispute (Burkina Faso/Republic of Mali), (1986) ICJ Rep 554

Case concerning the Gabčikovo-Nagymaros Project (Hungary v Slovakia), (1997) ICJ Rep 7

Case concerning the Temple of Preah Vihear (Cambodia v Thailand), Merits, (1962) ICJ Rep 6

Case concerning United States Diplomatic and Consular Staff in Tehran (United States of America v Iran), Merits, (1980) ICJ Rep 3

Case of al-Skeini and Others v. The United Kingdom, (Application no. 55721/07) 7 July 2011, ECtHR Grand Chamber, ECtHR 55721/07

Case of Observer and Guardian v. the United Kingdom, ECtHR 13585/88

Case of the Monetary Gold Removed from Rome in 1943 (Italy v France, United Kingdom and United States of America), (1954) ICJ Rep 19

Case of the S.S. 'Lotus' (France v. Turkey), (1927) PCIJ Rep Series A No 10

Case of the S.S. 'Wimbledon' (United Kingdom, France, Italy and Japan), (1923) PCIJ Rep Series A No 1

China – Measures Related to the Exportation of Various Raw Materials, WTO Appellate Body Report (2012) WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R

CMS Gas Transmission Company v. Argentine Republic, (2005) ICSID, ARB/01/8

Comcast v FCC, (2010) 600 F.3d 642

Continental Casualty Company v. Argentine Republic, (2008) ICSID, ARB/03/9

Corn Products International v. Mexico, Decision on Responsibility, (2008) ICSID, ARB(AF)/04/05

Crosby v Cox Aviation Co. of Washington 746 P.2d 1198 (Wash 1987)

Delfi AS v Estonia, ECtHR 64569/09

Dominican Republic – Measures Affecting the Importation and Internal Sale of Cigarettes, (2005) WT/DS302/AB/R

East Timor (Portugal v Australia), (1995) ICJ Rep 90

*Eastern Airlines vs Flo*yd, 499 US 530, (S. Ct. 1991) 533

EC—Asbestos, WTO, (2001) WT/DS135/AB/R

Effects of Awards of Compensation made by the United Nations Administrative Tribunal, Advisory Opinion, (1954) ICJ Rep 54

Electricity Company of Sofia and Bulgaria (Belgium v Bulgaria), Order, (1939) PCIJ Rep Series A/B No 79

Eritrea Ethiopia Claims Commission, Partial Award: *Jus Ad Bellum* (Ethiopia's Claims 1-8), EECC, 19 December 2005

Gardel v. France, (2005) ECtHR 16428/05

Greco-Bulgarian 'Communities', Advisory Opinion, (1930) PCIJ Rep Series B No 17

Haddad c. Air France, 1982 RFDA XXXIII Année 1979 327

Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt, Advisory Opinion, (1980) ICJ Rep 73

Island of Palmas (Netherlands v United States of America), (1928) 2 R.I.A.A. 829

Italy v Commission, (1985) 2 CMLR 368, 373

Janes Case (United States of America v Mexico), (1925) IV R.I.A.A. 82

Japan – Measures affecting the purchase of telecommunications equipment, 18 August 1995, WTO WT/DS15

Jurisdictional Immunities of the State (Germany v Italy; Greece Intervening), (2012) ICJ Rep 37

Korea – Laws, regulations and practices in the telecommunications procurement sector, 5 May 1996, WTO WT/DS40

Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef, (2005) WT/DS161/AB/R

Lac Lanoux (France v Spain), (1957) 12 R.I.A.A. 281

LaGrand Case (Germany v United States of America), (2001) ICJ Rep 466

Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), Advisory Opinion, (1971) ICJ Rep 16

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, (2004) ICJ Rep 136

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, (1996) ICJ Rep 226

M.B. v. France, (2009) ECtHR 5335/06, 16428/05, 22115/06

M.K. v. France, (2013) ECtHR 19522/09

M/V 'Saiga' (No.2) (Saint Vincent and the Grenadines v Guinea), ITLOS Case No 2, ICGJ 336 (ITLOS 1999)

Mavrommatis Palestine Concessions (Greece v United Kingdom), (1924) PCIJ Rep Series A No 2

Mazzanti v *HAFSE and Ministry of Defence* (Tribunal of Florence, Italy, 2 January 1954), (1954) 22 ILR 758

MCI Communications v AT&T, 708 F 2d 1081 (7th Cir 1983), 464 US 891 (1983)

Mexico – Measures affecting Telecommunication Services, Report of the Panel, 2 April 2004, WT/DS204/R

Nationality Decrees in Tunis and Morocco, Decision, (1923) PCIJ Series B No 4

Naulilaa Arbitral Award (Portugal v Germany), (1928) 2 R.I.A.A 1011

North Sea Continental Shelf (Federal Republic of Germany v Denmark), (1969) ICJ Rep 3

Nottebohm Case (Liechtenstein v Guatemala), (1955) ICJ Rep 4

Nuclear Tests (Australia v France), (1974) ICJ Rep 253

Oil Platforms (Islamic Republic of Iran v United States of America), Merits, (2003) ICJ Rep 161

Olympic Airways v Husain 540 US 644, (S. Ct. 2004) 12

Phosphates in Morocco (Italy v France), Preliminary Objections, (1938) PCIJ Rep Series A/B No 74

Prosecutor v Dusko Tadic (Appeals Judgment), (1999) ICTY IT-94-1-A

R v Sheppard & Anor, (2010) EWCA Crim 65 (UK)

R. v M.A.F.F, ex parte Hedley Limited (Ireland), Case C5/94, (1996) R.C.R. I-2553

Reno v ACLU, (1997) 521 US 844

Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide, Advisory Opinion, (1951) ICJ Rep 15

Responsabilité de l'Allemagne à raison des dommages causés dans les colonies portugaises du sud de l'Afrique (Portugal v Germany), (1928) II R.I.A.A. 1011

Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area, Advisory Opinion in Case No 17, (2011) ITLOS, Seabed Disputes Chamber

Rotaru v. Romania, (2000) ECtHR 28341/95

S. and Marper v the UK, (2008) ECtHR 30562/04; 30566/04

Sambaggio Case (Italy v Venezuela), (1903) X R.I.A.A. 499

Segerstedt-Wiberg and Others v Sweden, (2006) ECtHR 62332/00

Sempra Energy International v Argentine Republic, (2007) ICSID, ARB/02/16

South West Africa (Ethiopia v South Africa; Liberia v South Africa), Second Phase, (1966) ICJ Rep 5

Southern Bluefin Tuna Cases (New Zealand v Japan; Australia v Japan), Provisional Measures, (1999) ITLOS Cases Nos 3, 4

South-West Africa Voting Procedure, Advisory Opinion, (1955) ICJ Rep 67

State of the Netherlands v *Hasan Nuhanovic*, Netherlands Supreme Court, (2013) 12/02234

Tadić, 15 July 1999, ICTY, Appeals Chamber, Case no IT-94-1-A

Teichner v Air France Airlines, (1987) IsrSC 41(1) 589

Territorial and Maritime Dispute (Nicaragua v Colombia), (2012) ICJ, Jugement of 19 November 2012

Territorial Jurisdiction of the International Commission of the River Oder (United Kingdom, Czechoslovakia, Denmark, France, Germany, Sweden v Poland), (1929) PCIJ Rep Series A No 16

The Corfu Channel Case (United Kingdom v Albania), Merits, (1949) ICJ Rep 4

The Trail Smelter Arbitration Case (United States of America v Canada), (1938) 3 R.I.A.A. 1905

United States – Import Prohibition of Certain Shrimp and Shrimp Products, WTO, (1998) WT/DS58/AB/R

United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WTO, (2005) WT/DS285/AB/R

United States – Measures Affecting the Production and Sale of Clove Cigarettes, WTO, (2012) WT/DS406/AB/R

Van der Velden v. The Netherlands, (2006) ECtHR 21203/10

Velásquez Rodríguez Case, Inter-American Court of Human Rights, (1988) Series C No 4

Western Sahara, Advisory Opinion, (1975) ICJ Rep 12

Yeager v Islamic Republic of Iran, (1987) U.S.C.T.R 17

Youmans Case (United States v Mexico), (1926) IV R.I.A.A. 1100

International Treaties and Agreements

Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (2009)

Agreement Establishing the World Trade Organisation (1994)

Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1979)

Agreement On The Prevention Of Dangerous Military Activities concluded between Canada and USSR (1991)

Agreement On The Prevention Of Dangerous Military Activities concluded between the US and the USSR (1989)

Agreement on the Prevention of Incidents On and Over the Waters Outside the Limits of the Territorial Sea (1972) (as Amended by the 1973 Protocol to the Agreement and the 1998 Exchange of Diplomatic Notes between the US and the USSR)

Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched Into Outer Space (1967)

Agreement relating to the Implementation of Part XI of the United Nations Convention on the Law of the Sea of 10 December 1982 (1994)

American Convention on Human Rights (1969)

Charter of Fundamental Rights of the European Union (2000)

Charter of the Organization of African Unity (1963)

Charter of the Organization of American States (1948)

Charter of the United Nations (1945)

Consolidated Version of the Treaty of the Functioning of the EU (2010)

Constitution of the International Telecommunication Union (1992)

Constitution of the World Health Organization (1946)

Constitutive Act of the African Union (2000)

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949)

Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (1949)

Convention (III) Relative to the Treatment of Prisoners of War (1949)

Convention (IV) Relative to the Protection of Civilian Persons in Time of War (1949)

Convention for the Protection of Human Rights and Fundamental Freedoms (1950)

Convention for the Protection of Submarine Telegraph Cables (1884)

Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1973)

Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988)

Convention for the Suppression of Unlawful Seizure of Aircraft (1970)

Convention for the Unification of Certain Rules for International Carriage by Air (2003)

Convention for the Unification of Certain Rules relating to Damage Caused by Foreign Aircraft to Third Parties on the Surface (1933)

Convention for the Unification of Certain Rules Relating to International Carriage by Air (1933)

Convention of the International Telecommunication Union (1992)

Convention on Compensation for Damage to Third Parties Resulting from Acts of Unlawful Interference Involving Aircraft (2009)

Convention on Cybercrime (2001)

Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface (1952)

Convention on Diplomatic Officers (1928)

Convention on Early Notification of a Nuclear Accident (1986)

Convention on International Civil Aviation (1944)

Convention on International Liability for Damage Caused by Space Objects (1972)

Convention on Private International Law (1928)

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (1980)

Convention on Registration of Objects Launched into Outer Space (1975)

Convention on Relations of States with International Organizations (1975)

Convention on Rights and Duties of States (inter-American) (1933)

Convention on Special Missions (1969)

Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents (1973)

Convention on the Privileges and Immunities of the Specialized Agencies (1947)

Convention on the Privileges and Immunities of the United Nations (1946)

Convention on the Protection and Use of Transboundary Watercourses and International Lakes (1936)

Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (2010, not yet in force)

Convention on Third Party Liability in the Field of Nuclear Energy (1960)

European Convention on Human Rights (1950)

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field (1929)

Geneva Convention on the Continental Shelf (1958)

Geneva Convention on the High Seas (1958)

Hague Regulations Respecting the Laws and Customs of War on Land (1907)

International Convention Against the Taking of Hostages (1979)

International Convention on Civil Liability for Oil Pollution Damage (1969)

International Convention on Telecommunications (1947)

International Covenant on Civil and Political Rights (1966)

International Covenant on Economic, Social and Cultural Rights (1966)

NATO Status of Forces Agreement (1951)

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (1977)

Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971)

Protocol on Environmental Protection to the Antarctic Treaty (1991)

Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II) (1980)

Protocol on the Status of International Military Headquarters set up Pursuant to the North Atlantic Treaty (1952)

Protocol Relating to Fixed Platforms Located on the Continental Shelf (1988)

Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (2010, not yet in force)

Protocol to Amend the Convention on Damage Caused by Aircraft to Third Parties on the Surface (1978)

Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005)

Protocol to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platform Located on the Continental Shelf of 1988 (2005)

Statute of the International Court of Justice (1945)

Statute of the International Criminal Court (1998)

Statute of the Permanent Court of International Justice (1920)

Strategic Arms Limitation Treaty (SALT I) (1972)

Strategic Arms Limitation Treaty (SALT II) (1991)

The Antarctic Treaty (1959)

The United Nations Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea (1982)

Treaty between the United States of America and the Argentine Republic concerning the Reciprocal Encouragement and Protection of Investment (1991)

Treaty of Amity and Cooperation in Southeast Asia (1976)

Treaty of Amity, Economic Relations, and Consular Rights Between the United States of America and Iran (1955)

Treaty on Open Skies (1992)

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (1967)

Treaty on the Elimination of Intermediate-Range and Shorter Range Missiles (1987)

Treaty on the Limitation of Anti-Ballistic Missile Systems (1972)

Treaty on the Non- Proliferation of Nuclear Weapons (1968)

Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof (1971)

Understanding on rules and procedures governing the settlement of disputes (Annex 2 to the Agreement Establishing the World Trade Organization) (1994)

United Nations Convention on the Law of the Sea (1982)

United Nations Convention to Combat Desertification in Those Countries Experiencing Serious Drought and/or Desertification, Particularly in Africa (1994)

Vienna Convention on Consular Relations (1963)

Vienna Convention on Diplomatic Relations (1961)

Vienna Convention on the Law of Treaties (1969)

International Instruments

African Union, 'Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa' (2012) <http://au.int/en/cyberlegislation>

African Union, 'Protocol Relating to the Establishment of the Peace and Security Council of the African Union' (Durban, 9-10 July 2002) <http://www.au.int/en/content/protocol-relating-establishment-peace-and-security-council-african-union>

Council of the European Union Decision 2012/168/CFSP amending Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in Iran (23 March 2012)

Council of the European Union Decision 2012/36/CFSP of 23 January 2012 amending Decision 2010/639/CFSP concerning restrictive measures against Belarus

European Union Council Regulation (EC) No. 3286/94 of 22 December 1994laying down Community procedures in the field of the common commercial policy in order to ensure the exercise of the Community's rights under international trade rules, in particular those established under the auspices of the World Trade Organization (OJ L 349/71)

European Union Directive (EC), 'Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC', COM (2007) 697

European Union Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178/1, 17 July 2000)

European Union Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (OJ L 108/33, 24 April 2002)

European Union Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (OJ L 337/11, 18 December 2009)

European Union Directive 2010/13/EU 'on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services' (OJ L 95/1, 14 April 2010)

European Union Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, (OJ 2013 L 218/8, 14 August 2013)

European Union Directive 99/5/EC on radio and telecommunications terminal equipment (OJ L91/10, 7 April 1999)

European Union Regulation (EC) No 29/2009 of 16 January 2009 laying down requirements on data link services for the single European sky

European Union Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005

European Union Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the Single European Sky (Framework Regulation) and Statement by the Member States on military issues related to the Single European Sky (attached to Regulation (EC) No 549/2004)

European Union Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the Interoperability Regulation)

European Union Regulation (EC) No. 216/2008 of the European Parliament and of the Council of 20 February 2008 concerning on common rules in the field of civil aviation and establishing a European Aviation Safety Agency

European Union Regulation (EC) No. 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (OJ L 162/40, 30 April 2004)

European Union Regulation No. 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain (OJ L 113/1, 30 April 2002)

European Union, European Commission, *A Digital Agenda for Europe - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (EU 26 August 2010) COM/2010/0245 f/2 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT>

European Union, European Commission, *European Public-Private Partnership for resilience – EP3R* (EU 2010) <http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm>

European Union, European Commission, *Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent* (COM(2013) 627 final, 0EU (2013)

European Union, European Defence Agency, *Diplomatic Clearance Technical Arrangement* (19 December 2012)

Inter-Agency Space Debris Coordination Committee (IADC), 'Space Debris Mitigation Guidelines' UN Doc. A/AC.105/C.1/L.260 (2002)

International Cable Protection Committee (ICPC), 'Actions for Effective Cable Protection (Post Installation)' (ICPC Recommendation No. 6, Issue 8A, 2008)

International Civil Aviation Organisation (ICAO), 'Global Air Traffic Management Operational Concept' (ICAO Doc. 9854)

International Civil Aviation Organisation (ICAO), 'ICAO Procedures of Air Navigation Services' (PANS-ATM, ICAO Doc. 4444)

International Civil Aviation Organisation (ICAO), 'Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference' (ICAO Doc. 8973/8) – access restricted

International Civil Aviation Organization (ICAO), 'Working Paper to the Twelfth Air Navigation Conference' (19 to 30 November 2012, AN-Conf/12-WP/122)

International Law Commission, 'Articles concerning the Law of the Sea with commentaries' (YBILC 256 1956 II)

International Law Commission, 'Commentary on the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities' (Report of the ILC on its 53rd Session, UN Doc. A/56/10, 2001)

International Law Commission, 'Draft Articles on Prevention of Transboundary Harm from Hazardous Activities' (A/RES/56/10 ILC)

International Law Commission, 'Draft articles on Responsibility of States for Internationally Wrongful Acts' (UN Doc A/RES/56/83 12, 2001, annex)

International Law Commission, 'Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law' (Report of the Study Group of the International Law Commission, finalised by Martti Koskenniemi, UN Doc No A/CN.4/L.682, 2006)

International Law Commission, Responsibility of International Organizations (UN Doc. A/CN.4/L.778, 30 May 2011)

International Organisation for Standardization, 'Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model' (1994) <http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip>

International Organisation for Standardization, 'Information technology - Security techniques - Information security management systems - Requirements' (2013) <http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534>

International Organization for Standardization, 'Information technology — Security techniques — Information security management systems — Overview and vocabulary' (1 May 2009) <http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip>

International Telecommunication Union, *Handbook on Satellite Communications* (ITU 2002)

International Telecommunications Union, 'Final Acts of the World Conference on International Telecommunications' (Dubai, 2012) <http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf>

International Telecommunications Union, 'ITU World Radiocommunications Conference concludes after four weeks: International treaty sets future course for wireless' (Press Release WRC-07, 16 November 2007)

International Telecommunications Union, Reform Advisory Panel (RAP), *Observations and Recommendations for Reform*, 10 March 2000

International Telecommunications Union, *Resolution 79* (Minneapolis, 1998)

International Telecommunications Union, *Resolution 110* (Marrakesh, 2002)

International Telecommunications Union, *Resolution 121* (Marrakesh, 2002)

International Telecommunications Union, *Resolution 146* (Antalya, 2006)

International Telecommunications Union, *Resolution 179* (Guadalajara, 2010)

International Telecommunications Union, *Technical framework for countering email spam*, X.1241 (04/2008)

La Rue F, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (UN Doc. A/HRC/17/27, 16 May 2011)

La Rue F, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (UN Doc. A/HRC/23/40, 17 April 2013)

La Rue F, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (UN GA Doc. A/66/290, 10 August 2011)

La Rue F, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (UN Doc. A/HRC/23/40, 13 April 2013)

North Atlantic Treaty Organization, *Allied Joint Doctrine for Information Operations (Allied Joint Publication AJP-3.10, NATO/PfP UNCLASSIFIED*, (NATO November 2009) <http://info.publicintelligence.net/NATO-IO.pdf>

North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 'NATO Glossary of Terms and Definitions' (AAP-6 of 2008), (NSA, 2013) <http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf>

North Atlantic Treaty Organization, Standardization Agreement (STANAG) 4586 for Standard Interfaces of UAV Control System (UCS) <http://nsa.nato.int/nsa/nsdd/listpromulg.html>

North Atlantic Treaty Organization, Standardization Agreement (STANAG), 'STANAG 5501: Digital Data Link 1 (Point to Point) <http://nsa.nato.int/nsa/nsdd/listpromulg.html>

North Atlantic Treaty Organization, Standardization Agreement (STANAG), 'STANAG 5511: Tactical Data Exchange - Link 11 <http://nsa.nato.int/nsa/nsdd/listpromulg.html>

North Atlantic Treaty Organization, Standardization Agreement (STANAG), 'STANAG 5516: Tactical Data Exchange - Link 16 <http://nsa.nato.int/nsa/nsdd/listpromulg.html>

North Atlantic Treaty Organization, Strategic Concept for the Defence and Security (Lisbon, 19 November 2010) <http://www.nato.int/cps/en/natolive/official_texts_68580.htm#cyber>

Organisation for Economic Co-operation and Development, 'Guidelines for the Security of Information Systems' (OCDE/GD(92)190, 1992)

Organisation for Economic Co-operation and Development, 'The Multilateral Agreement on Investment' (Draft Consolidated Text, DAFFE/MAI(98)7/REV1, 22 April 1998) <http://www1.oecd.org/daf/mai/pdf/ng/ng987r1e.pdf>

Organization for Security and Co-operation in Europe, 'Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (PC.DEC/1039, 2013)

Organization for Security and Co-operation in Europe, 'Resolution on the Overall Approach of the OSCE to Promoting Cybersecurity in OSCE, Resolutions of the OSCE Parliamentary Assembly Adopted at the Twentieth Annual Session' (AS (11) R E, Belgrade 6 to 10 July 2011)

Organisation for Security and Co-operation in Europe, 'The Final Act of the Conference on Security and Cooperation in Europe' (Helsinki Declaration, 14 ILM 1292, 1978)

Organization for Security and Co-operation in Europe, 'Vienna 2011 Document on Confidence- and Security-Building Measures (CSBMs)' (FSC.DOC/1/11, 2011)

Organization of American States, 'Declaration by the Experts on Confidence- and Security-Building Measures: Recommendations to the Summit-Mandated Special Conference on Security' (OEA/Ser.K/XXIX, RESEGRE/doc.4/03 rev 3, 2003)

Organization of American States, 'Declaration of San Salvador on Confidence- and Security-Building Measures' (OEA/Ser.K/XXIX.2, COSEGRE.II/doc.7/98 rev 3, 1998)

Organization of American States, 'Declaration of Santiago on Confidence- and Security-Building Measures' (OEA/Ser.K/XXIX.2, COSEGRE/doc.18/95 rev 3, 1995)

Organization of American States, Permanent Council, Committee on Hemispheric Security, 'Consolidated List of Confidence and Security Building Measures for Reporting according to OAS Resolutions' (Approved 15 January 2009) <http://www.oas.org/csh/english/csbmlist.asp#Santiago>

United Nations Commission on Human Rights, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (UN Doc. E/CN.4/1985/4, Annex, 28 September 1984) <http://www1.umn.edu/humanrts/instree/siracusaprinciples.html>

United Nations Committee on Economic, Social and Cultural Rights, 'General Comment 8, The Relationship Between Economic Sanctions and Respect for Economic, Social and Cultural Rights' (Seventeenth session, 1997, UN Doc. E/C.12/1997/8 (1997)

United Nations Conference on Environment and Development (3–14 June 1992, UN Doc. A/CONF.151/26/Rev.1, vol I)

United Nations Conference on the Law of the Sea, 'Official Records' (vol IV, Geneva, 24 February – 27 April 1958)

United Nations General Assembly, 'Combating the criminal misuse of information technologies' (A/RES/55/63, 2001; 56/121, 2002)

United Nations General Assembly, 'Creation of a Global Culture of Cybersecurity' (A/RES/57/239, 2002)

United Nations General Assembly, 'Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures' (A/RES/58/199, 2003)

United Nations General Assembly, 'Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures' (A/RES/64/211, 2009)

United Nations General Assembly, 'Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space' (A/RES/18/1962, 1963)

United Nations General Assembly, 'Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries' (A/RES/51/122, 1996)

United Nations General Assembly, 'Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Friendly Relations Declaration)' (A/RES/2625 (XXV), 1970)

United Nations General Assembly, 'Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations' (A/RES/42/22, 1987)

United Nations General Assembly, 'Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States' (A/RES/36/103, 1981)

United Nations General Assembly, 'Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty' (A/RES/2131 [XX], 1965)

United Nations General Assembly, 'Developments in the Field of Information and Telecommunications in the Context of International Security' (A/RES/53/70, 1998; A/RES/54/49, 1999; A/RES/55/28, 2000; A/RES/56/19, 2001; A/RES/57/53, 2002; A/RES/58/32 2003; A/RES/59/61, 2004; A/RES/60/45, 2005; A/RES/61/54, 2006; A/RES/62/17, 2007; A/RES/63/37, 2008; A/RES/64/25, 2009; A/RES/65/41, 2010; A/RES/66/24, 2011; A/RES/67/27, 2012)

United Nations General Assembly, 'International Co-operation in the Peaceful Uses of Outer Space' (A/RES/1721 (XVI), 1961)

United Nations General Assembly, 'International Cooperation on the Peaceful Uses of Outer Space' (A/RES/62/217, 2008)

United Nations General Assembly, 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (A/RES/66/359, 2011)

United Nations General Assembly, 'Prevention of an Arms Race in Outer Space: Study on the Application of Confidence-Building Measures in Outer Space' (A/RES/48/305, 1993)

United Nations General Assembly, 'Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting' (A/RES/37/92, 1982)

United Nations General Assembly, 'Principles Relating to Remote Sensing of the Earth from Outer Space' (A/RES/41/65, 1986)

United Nations General Assembly, 'Principles Relevant to the Use of Nuclear Power Sources in Outer Space' (A/RES/47/68, 1992)

United Nations General Assembly, 'Resolution Relating to the Information to be Furnished by States about the Malfunctioning of NPS in Outer Space' (A/RES/33/16, 1978)

United Nations General Assembly, 'Strengthening the United Nations Crime Prevention and Criminal Justice Programme' (A/RES/63/195, 2008; A/RES/64/179, 2009; A/RES/65/232, 2011)

United Nations General Assembly, 'The promotion, protection and enjoyment of human rights on the Internet' (UN Doc No A/HRC/20/L.13)

United Nations General Assembly, 'United Nations Millennium Declaration' (A/RES/55/2, 2000)

United Nations Human Rights Committee, 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988)

United Nations Human Rights Committee, 'General Comment No. 31 (80) Nature of the General Legal Obligation Imposed on States Parties to the Covenant' (ICCPR document CCPR/C/21/Rev.1/Add.13, 26 March 2004)

United Nations Human Rights Council, 'General Comment No. 34 – Freedom of opinion and expression' (ICCPR document CCPR/C/GC/34, 12 September 2011)

United Nations Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet' (UN Human Rights Council 20th session, UN Doc. A/HRC/20/L.13, 29 June 2012)

United Nations Security Council Resolution 1267 (15 October 1999)

United Nations Security Council Resolution 1333 (19 December 2000)

United Nations Security Council Resolution 1368 (12 September 2001)

United Nations Security Council Resolution 1373 (28 September 2001)

United Nations, 'The right to privacy in the digital age' (Brazil and Germany, draft resolution UN Doc. A/C.3/68/L.45, 1 November 2013)

Statute Law

Australia

Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Act (2005)

Federal Republic of Germany

Act on the Privatization of Shares of Volkswagenwerk Gesellschaft mit beschränkter Haftung (1960)

Malaysia

Continental Shelf Act, Act No. 83 (1972)

Continental Shelf Act, Act No. 57 (1996)

New Zealand

Submarine Cables and Pipeline Protection Act, Act No. 22 (1996)

People's Republic of China

Constitution of the People's Republic of China' (2004)

South Korea

Act on Promotion of Information and Communications Network Utilization and Information Protection (2002)

United Kingdom

Communications Act (2003)

The Telephone Number Exclusion (Domain Names and Internet Addresses) Order (2003)

United States

Air Transportation Safety and System Stabilization Act (2001)

Constitution of the United States (1787)

Economic Espionage Act (1996)

Electronic Communications Privacy Act (1986)

Foreign Intelligence Surveillance Amendments Act (2008)

Uniform Aviation Liability Act (1922)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ('The Patriot Act') (2001)

Statements and Presentations

Alexander Gen K, 'U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM' (transcript of an address at the Center for Strategic and International Studies, 3 June 2010) <http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf>

Association of Southeast Asian Nations Regional Forum, 'The Chairman's Statement of the Twentieth ASEAN Regional Forum' (Bandar Seri Begawan, Brunei Darussalam, 2 July 2013) <http://aseanregionalforum.asean.org/library/arf-chairmans-statements-and-reports.html>

Association of Southeast Asian Nations, 'ASEAN ICT Masterplan 2015' (1 January 2011) <http://www.asean.org/resources/publications/asean-publications/item/asean-ict-masterplan-2015>

Association of Southeast Asian Nations, 'Chairman's Statement of the 19th ASEAN Regional Forum' (Phnom Penh, Cambodia 12 July 2012) <http://aseanregionalforum.asean.org/library/arf-chairmans-statements-and-reports.html>

Bennett G, 'A Look at the Soviet Space Nuclear Power Program' (NASA, Energy Conversion Engineering Conference 1989)

China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS), 'Joint Statement. Bilateral Discussions on Cooperation in Cybersecurity' (June 2012) <http://csis.org/files/attachments/120615_JointStatement _CICIR.pdf>

Clapper J R, 'Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence' (31 January 2012) <http://www.intelligence.senate.gov/120131/clapper.pdf>

Communications from Australia, Canada, the European Communities, Japan, Hong Kong China, Korea, Norway, Singapore, the Separate Customs Territory of Taiwan, Penghu, Kinmen, and Matsu and the United States (1 July 2005 ,WTO TN/S/W/50)

European Air Safety Agency, 'Policy Statement – Airworthiness Certification Policy of Unmanned Aircraft Systems (UAS)' (Doc. E.Y013-01, 25 August 2009)

European Commission High Representative of the European Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (Brussels, 7 February 2013, JOIN(2013) 1)

Federal Republic of Germany, Foreign Office 'Cyber security: confidence and security-building measures (CSBMs)' (undated) <http://www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung_/KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html>

Federal Republic of Germany, Informationstechnik, Bundesamt für Sicherheit in der, 'IT-Grundschutz' (2013) <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html>

Federal Republic of Germany, Permanent Mission to the United Nations, 'Note to the United Nations, New York' (Note Verbale/Note No. 516/2012, November 2012) <http://www.un.org/disarmament/topics/informationsecurity/docs/Germany_Verbal_Note_516_UNODA.pdf>

Fedosov S, 'Statement by the Russian participant at the UNIDIR Cyber Security Conference "What does a Stable Cyber Environment Look Like?"' (UNIDIR, Geneva, 8-9 November 2012) <http://www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf>

Group of 8, 'Deauville G8 Declaration, Renewed Commitment for Freedom and Democracy' (Deauville 26-27 May 2011)

Hague W, 'Security and freedom in the cyber age - seeking the rules of the road' (Speech delivered on 4 February 2011 at the Munich Security Conference) <https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road>

Hague W, 'The Rt Hon William Hague MP, London Conference on Cyberspace: Chair's Statement' (2 November 2011) <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement>

ICANN *et al*., Montevideo Statement on the Future of Internet Cooperation (7 October 2013) <http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm>

Japan, Ministry of Internal Affairs and Communications, 'Collaboration between Japan and Malaysia concerning Proactive Response Against Cyber-attacks Through International Collaborative Exchange ("PRACTICE")' (Press Release 7 March 2013) <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130307_02.html>

Koh HH, 'International Law in Cyberspace' 18 September 2012 (speech) <http://www.State.gov/s/l/releases/remarks/197924.htm>

Lisbon European Council 23 and 24 March 2000 Presidency Conclusions <http://www.europarl.europa.eu/summits/lis1_en.htm>

Mallery JC, 'A Strategy for Cyber Defense' (earlier title: Multi-spectrum Evaluation Frameworks and Metrics for Cyber Security and Information Assurance, Presented at the MIT/Harvard Cyber Policy Seminar, 2011)

Ministry of Foreign Affairs of Japan, 'ASEAN Regional Forum: Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security' (Phnom Penh, 12 July 2012) <http://www.mofa.go.jp/files/000016403.pdf>

Ministry of Internal Affairs and Communications of Japan, 'Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation' (Tokyo, 13 September 2013) <http://www.soumu.go.jp/main_content/000249127.pdf>

Netherlands, 'Government response to the AIV/CAVV report on cyber warfare' (Statement of 17 January 2012) <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf>

Organisation for Economic Co-operation and Development, 'G20 Leader's Statement, the Pittsburgh Summit' (24-25 September 2009) <http://www.oecd.org/g20/meetings/pittsburgh/>

Sweden, 'General statement in connection with action on L.30 Developments in the field of information and telecommunications in the context of international security' (6 November 2012) <http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com12/statements/L30_Sweden-joint.pdf>

Sweden, Ministry of Foreign Affairs, 'Enhancing Internet freedom and human rights through responsible business practices' (13 April 2012) <http://www.government.se/content/1/c6/19/05/60/591bf7d9.pdf>

United States of America, 'Comments on the Draft Articles on State Responsibility', (1998) 37 *International Law Materials* 468

United States of America, The White House, 'Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin, U.S. and Russian Delegations Meet to Discuss Confidence-Building Measures in Cyberspace' (23 June 2011) <http://www.whitehouse.gov/sites/default/files/uploads /2011_klimashin_schmidt_cyber_joint_statement.pdf>

United States of America, The White House, 'Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building' (17 June 2013) <http://www.whitehouse.gov/the-press-office/2013/06/17/joint-statement-on-a-new-field-of-cooperation-in-confidence-building>

United States of America, The White House, 'U.S.-Russian Cooperation on Information and Communications Technology Security' (Factsheet, 2013) <http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>

WTO Ministerial Declaration, 14 November 2001 (WT/MIN(01)/DEC/1)

Yankey A, 'Presentation at the Commonwealth Cybersecurity Forum 2013' (African Union Commission, 22-26 May 2013) <http://www.cto.int/events/previous-events/cto-past-events-2013/commonwealth-cybersecurity-forum-2013/commonwealth-cybersecurity-forum-2013-presentations/>

Websites

African Union, 'Cyber Security' <http://pages.au.int/infosoc/pages/cyber-security>

Black Hat, 'Black Hat - About' (2013) <https://www.blackhat.com/html/about.html>

Centre for the Protection of National Infrastructure, 'Overview of CPNI' (2013) <http://www.cpni.gov.uk/>

Council of Europe, 'Convention on Cybercrime – Status' (2013) <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>

Council of Europe, 'Cybercrime' <http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp>

CSTO, 'Basic Facts' <http://www.odkb.gov.ru/start/index_aengl.htm>

Electronic Frontier Foundation, 'About EFF' (2013) <https://www.eff.org/about>

Estonian Defence League, 'Estonian Defence League's Cyber Unit' (2013) <http://www.kaitseliit.ee/en/cyber-unit>

EUR Lex 'Access to European Law' <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>

European Space Agency, 'Space Debris Evolution in Pictures' <http://www.esa.int/About_Us/ESOC/Space_debris_-_evolution_in_pictures>

European Union Agency for Network and Information Security, 'National Cyber Security Strategies' (2013) <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>

European Union, EC-Council, 'EC-Council - About CEH v8' (2013) <https://www.eccouncil.org/Certification/certified-ethical-hacker>

Forum for Incident Response and Security Teams, 'FIRST' <http://www.first.org/>

Google, 'IPv6 Statistics' (2013) <http://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption>

International Telecommunication Union, 'Members of the Reform Advisory Panel' <http://www.itu.int/newsroom/reform/rapmembers.html>

Information Warfare Monitor, <http://www.infowar-monitor.net/>

International Cable Protection Committee, <http://www.iscpc.org>

International Telecommunication Union, 'Global Cybersecurity Agenda' <http://www.itu.int/osg/csd/cybersecurity/gca/>

International Telecommunication Union, 'ICT Facts and Figures' (2013) <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>

International Telecommunication Union, 'ITRs' <http://www.itu.int/ITU-T/itr/files/ITR-e.doc>

International Telecommunication Union, 'Sector Membership' <http://www.itu.int/en/membership/Pages/sector-members.aspx>

Internet Assigned Numbers Authority, 'IANA IPv4 Address Space Registry' (20 May 2013) <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>

Internet Assigned Numbers Authority, 'IANA Number Resources' <http://www.iana.org/numbers>

Internet Assigned Numbers Authority, 'IANA WHOIS Service' <http://www.iana.org/whois>

Internet Corporation for Assigned Names and Numbers and US Department of Commerce, 'Contracts on IANA Functions' <http://www.icann.org/en/about/agreements>

Internet Corporation for Assigned Names and Numbers, 'ICANN Factsheet' <http://archive.icann.org/en/factsheets/fact-sheet.html>

Internet Engineering Task Force, 'About the IETF' (2013) <http://www.ietf.org/about/>

Internet Engineering Task Force, 'IP Version 6 Working Group' <http://datatracker.ietf.org/wg/ipv6/charter/>

Internet Society, 'IPv6' <http://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6>

Internet Society, 'World IPv6 Launch' <http://www.worldipv6launch.org/>

Kurbalija J, Evolution of technology and diplomacy, a series of blogs and webinars on the interplay between communication technology and diplomacy (2013) <http://www.diplomacy.edu/2013/evolution>

NASA, 'Apollo 13 Command and Service Modules' <http://nssdc.gsfc.nasa.gov/nmc/masterCatalog.do?sc=1970-029A>

NATO CCD COE, 'National Strategies & Policies' <http://ccdcoe.org/328.html>

NMAP, 'Security Scanner' <http://www.nmap.org>

North Atlantic Treaty Organization News, 'Developing NATO's cyber defence policy' (25 January 2011) <http://www.nato.int/cps/en/natolive/news_70049.htm>

North Atlantic Treaty Organization, 'A-Z: Crisis management' <http://www.nato.int/cps/ar/natolive/topics_49192.htm>

North Atlantic Treaty Organization, 'NATO and cyber defence' (2010) <http://www.nato.int/cps/en/SID-12A1F016-A72FF943/natolive/topics_78170.htm>

Organisation of American States, 'Confidence Building' <http://www.oas.org/csh/english/csbm.asp>

Organisation of American States, 'Cyber security program' (16 November 2011) <www.oas.org/cyber>

Organization for Security and Co-operation in Europe (OSCE), 'Cyber security: virtual threats, real responses' <http://www.osce.org/home/76011>

Organization for Security and Co-operation in Europe (OSCE), 'What is the OSCE?' <http://www.osce.org/secretariat/35775>

Organization for Security and Co-operation in Europe (OSCE), 'Who We Are' <http://www.osce.org/who>

Organization for Security and Co-operation in Europe, 'Confidence and Security Building' <http://www.osce.org/fsc/44569>

Riigi Infosüsteemi Amet, 'ISKE juhendid ja materjalid' (2011) <https://www.ria.ee/iske-dokumendid/>

The Hague Code of Conduct against Ballistic Missile Proliferation, 'What is HCOC?' <http://www.hcoc.at>

United Kingdom, Foreign and Commonwealth Office, 'Foreign Commonwealth Office Digital Diplomacy' <http://blogs.fco.gov.uk/digitaldiplomacy/>

United Nations Office for Disarmament Affairs, 'Confidence Building' <http://www.un.org/disarmament/convarms/infoCBM/>

United Nations Office for Disarmament Affairs, 'Small Arms and Light Weapons' <http://www.un.org/disarmament/convarms/SALW/>

United Nations Treaty Collection, 'Databases' <http://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10&chapter=18&lang=en>

United Nations, 'International Agreements and other Available Legal Documents Relevant to Space-Related Activities' (1999) <http://www.oosa.unvienna.org/pdf/spacelaw/intlagree.pdf>

United Nations, Treaties and Principles on Outer Space and Related General Assembly Resolutions <http://www.unoosa.org/oosa/en/SpaceLaw/treatystatus/index.html>

United States of America, Cyber Consequences Unit (2013) <http://www.usccu.us/>

United States of America, Department of Homeland Security, 'Cybersecurity' (2013) <http://www.dhs.gov/topic/cybersecurity>

United States of America, Federal Bureau of Investigation, 'Intellectual Property Theft' <http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr>

United States of America, Federal Bureau of Investigation, 'Quick Facts' (2013) <http://www.fbi.gov/about-us/quick-facts>

United States of America, State Department, 'Major Programmes of IRM's Office of eDiplomacy' <http://www.state.gov/m/irm/ediplomacy/c23840.htm>

Wealth Health Organization, 'About WHO' <http://www.who.int/about/en/>

Wealth Health Organization, 'What are the International Health Regulations?' <http://www.who.int/features/qa/39/en/index.html>

WTO Legal Texts <http://www.wto.org/english/docs_e/legal_e/legal_e.htm>

WTO Secretariat compilation <http://www.wto.org/english/tratop_e/serv_e/recap_e.xls>

WTO Telecommunication Services: <http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_coverage_e.htm#basic>

Authors´ Biographies

Liina Areng assumed the duties of International Relations Adviser in the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in October 2012. Prior to her current position she served as Senior Cybersecurity Adviser in the Ministry of Defence. From 2007 to 2010 Ms Areng worked as Assistant Defence Counsellor at the Permanent Representation of Estonia to NATO. Her previous positions include Arms Control Adviser at the Policy Planning Department (2005–2007) and Chief Expert on Russia and the Commonwealth of Independent States in the Defence Policy and Planning Department (2000–2005). She began her career in the Ministry in 1999. Liina Areng studied at St. Petersburg University in Russia and Oslo University in Norway, graduated from the University of Tartu in political science in 1999, and holds a Master's Degree in peace and conflict studies from the University of Jaume I in Spain. She has also worked as a research fellow in the NATO Defence College and participated in a variety of in-service training at the Swedish Defence College and at the NATO School in Oberammergau. Ms Areng has been awarded the Golden Cross of Services of the Ministry of Defence.

Oliver Aretz works since 2007 as Legal Assistant to the NATO Airborne Early Warning & Control Force, E-3A Component in Geilenkirchen, Germany. After completion of military service with the German Air Force, he studied law in Marburg and Münster, was admitted to practice law in 2006 and did so in the joint law offices in Aachen, Germany, focusing on criminal defense.

Emin Çalışkan is a Computer Scientist currently appointed as Turkey's Representative at NATO CCD COE. Prior to his assignment in the Research & Development Branch at the Center, he worked as a Penetration Tester and Cyber Security Researcher in the Scientific and Technological Research Council of Turkey (TUBITAK) - Cyber Security Institute (SGE). Mr Çalışkan holds Computer Engineering (2008) and Industrial Engineering (2009) bachelor degrees and continued his academic research in social sciences, receiving his Master's Degree from Bilgi University in Istanbul, Turkey in 2013 on Information and Technology Law. He is currently pursuing his PhD studies on the technical, political and legal aspects of nationwide offensive cyber security countermeasures at the Tallinn Technical University. He has been involved with numerous vulnerability assessment projects, both at the national and international level, focusing on information security risk management. Mr Çalışkan's current research areas include cyber security training and exercises, information security vulnerability assessments, penetration testing and offensive cyber defence studies, along with the strategic and legal aspects.

Major Dr Christian Czosseck has been with the German Army for more than 15 years. After his initial time as a cadet and later platoon commander in the NBC

branch, he became an IT professional and for the last 9 years has held different information assurance and IT management positions. Following his four-year tour (2008-2012) as scientist to the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), he is now serving at the Computer Emergency Response Team of the German Armed Forces (CERT Bundeswehr), part of the Bundeswehr Information Technology Center, and currently holds the position of Head of the *Cyber Defence Laboratory*. Major Czosseck holds a Ph.D. in Management from the Estonian Business School, Tallinn, and is a distinguished graduate in Computer Science from the Military University in Munich. His current research focus is on national cyber security and cyber weapons, with a particular focus on the role and use of botnets. He is editor of numerous conference proceedings, frequently serves as program committee member to cyber security related conferences, and lectures on cyber security and botnet related subjects, primarily at military venues. Major Czosseck has been appointed Ambassador to the NATO CCD COE.

Prof. Dr Chris C. Demchak has a PhD from the University of California Berkeley (political science) focused on organization theory and complex systems, security studies, and surprise in large-scale socio-technical systems across nations. She also holds two masters degrees in, respectively, economic development from Princeton and energy engineering from Berkeley. She has published numerous articles on societal security difficulties with large-scale information systems to include 'cybered conflict', national cyber power, and networked privacy, and is co-director of a recently established NWC Center for Cyber Conflict Studies (C3S). Dr. Demchak's recent books include an edited volume entitled *Designing Resilience* (U Pitt Press with Comfort and Boin, 2010) and a theory-to-practice volume *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security Conflicts* (UGA Press, 2011), as well as a prior book entitled *Military Organizations, Complex Machines* in the Cornell Security Studies series. She is currently working on a new manuscript tentatively entitled *Cyber Commands: Organizing For Cyber Security and Resilience in the Cybered Conflict Age*. As an early member of the Intelligence and Security Informatics (ISI) research field, she is also a board member of the Washington-based Cyber Conflict Studies Association (CCSA). Dr. Demchak currently conducts research and teaches graduate courses on cyber security and responses to surprise at the national and international level at the U.S. Naval War College.

Prof. Dr Robin Geiβ holds the Chair of International Law and Security at the University of Glasgow. Previously he was Professor of International and European Law at the University of Potsdam. Prior to that, he worked as Legal Adviser to the International Committee of the Red Cross (ICRC) in Geneva and as ICRC delegate to the United Nations Human Rights Council. At Glasgow, he convenes the LL.M. in International Law and Security. Professor Geiβ studied law in Bielefeld, Edinburgh, Kiel (PhD, 2005) and at the New York University (LL.M., 2004), and is a qualified German lawyer (admitted in 2007). His areas of research include most major subjects

of public international law, in particular United Nations law, statehood, human rights, international humanitarian and international criminal law. A former scholar of the German National Merit Foundation, Robin Geiβ is currently managing editor of the *Yearbook of International Humanitarian Law* and Rapporteur of the International Law Association's (ILA) Study Group on the challenges to international humanitarian law in contemporary armed conflicts. He is also a member of a European research consortium that investigates the unintended consequences of international counter-narcotic measures and was a member of the international group of experts that, under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, drafted the *Tallinn-Manual* on international law applicable to cyber-warfare. He is the author of *Failed States* (Duncker & Humblot, 2005) and co-author of *Piracy and Armed Robbery at Sea* (OUP, 2011) and has published in a wide range of scholarly journals.

Prof. Dr Terry Gill is Professor of Military Law at the University of Amsterdam and the Netherlands Defence Academy and was first Assistant and later Associate Professor of Public International Law at Utrecht University from 1985 to 2013. He is Director of the Research Program on the *Law of Armed Conflict and Peace Operations* at the Amsterdam Centre for International Law and of the Netherlands Research Forum on the *Law of Armed Conflict and Peace Operations (LACPO*). He teaches courses on international law relating to use of force and peace operations, international humanitarian law and military operational law at The University of Amsterdam, Utrecht University and the Netherlands Defence Academy. He has been visiting scholar at Columbia University and visiting research fellow at Cambridge University, Universidade de Coimbra, Universidad de Granada and the International Institute of Humanitarian Law in San Remo. Professor Gill is editor in chief of the *Yearbook of International Humanitarian Law* and member of the editorial boards of *The Military Law Review (Militair Rechtelijk Tijdschrift),* the *Journal of Armed Conflict & Security Law* and the *Journal of International Peacekeeping.* He is a member of the Board of Directors of *The International Society of Military Law and the Law of War* and member of the *Lieber Group of The American Society of International Law,* the *Netherlands Society of International Law,* the *International Criminal Law Network* and the Netherlands *Militair Rechtelijke Vereniging.* He was member of the Group of Experts which drew up the *Tallinn Manual on the Application of International Law to Cyber Warfare*.

Prof. Dr Wolff Heintschel von Heinegg holds the Chair of Public Law, especially Public International law, European Law and Foreign Constitutional Law, at the Europa-Universität Viadrina in Frankfurt (Oder), Germany. In the academic years 2003/2004 and 2012/2013 he was the Charles H. Stockton Professor of International Law at the U.S. Naval War College. He was among a group of international lawyers and naval experts who produced the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*. Professor Heintschel von Heinegg has been a member of several groups of experts working on the current state and progressive development of international humanitarian law, including the *Manual on Air and Missile Warfare* (2010) and the *Tallinn Manual on*

the International Law Applicable to Cyber Warfare. He is a widely published author of articles and books on public international law and German constitutional law.

Stefan A. Kaiser is Legal Advisor of NATO's AWACS operations (Airborne Early Warning & Control Force, E-3A Component) since 2002. From 1992 until 2002 he practiced law as in-house counsel in international corporations in the telecommunication and high-tech industry. He is a qualified German lawyer and aviator, holds an LL.M. from the McGill Institute of Air and Space Law and is a graduate of the International Space University. He lectures in air law at Leiden University and at the Aachen University of Applied Science.

Prof Dr Jan Klabbers holds degrees in international law and political science from the University of Amsterdam (1988), and obtained his doctorate in law from the same university (1996, with distinction). He taught international law, EU law and international relations at the University of Amsterdam from 1990 to 1996, and international law (including the law of international organizations) at the University of Helsinki since 1996. Between 2006 and 2011, he was director of the trans-disciplinary Centre of Excellence in Global Governance Research, funded by the Academy of Finland and located at the University of Helsinki. His main publications include *International Law* (2013), *An Introduction to International Institutional Law* (2nd ed., 2009), *Treaty Conflict and the European Union* (2008), *The Concept of Treaty in International Law* (1996) and, as co-author, *The Constitutionalization of International Law* (2009). He has held visiting positions in New York, Geneva and Paris, and has won several teaching awards. He holds the first Martti Ahtisaari Chair on behalf of the Academy of Finland since 2013, in order to work on a project on global ethics.

Dr Jovan Kurbalija is the Founding Director of DiploFoundation, a non-profit organisation working on diplomacy and digital politics. He is a Visiting Professor in e-diplomacy at the College of Europe in Bruges. A former diplomat, Dr Kurbalija has a professional and academic background in international law, diplomacy, and information technology. He has been a pioneer in the field of e-diplomacy since 1992 when he established the Unit for Information Technology and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. Dr Kurbalija has been an active participant in the global internet governance process as a member of the UN Working Group on Internet Governance (2003–2005) and special advisor of the Internet Governance Forum (2006–2011). He is a frequent contributor to international meetings and discussions on global digital policy. Dr Kurbalija's book, *An Introduction to Internet Governance*, is in its fifth edition and has been translated into eight languages. It is used as a textbook for academic courses on internet governance and digital politics worldwide. Dr Kurbalija lectures on e-diplomacy and internet governance in academic and training institutions in many countries, including Austria, Belgium, Switzerland, the United Kingdom, South Africa, and the United States.

Henning Lahmann studied law and philosophy in Hamburg and Prague and currently works as a research assistant at the University of Potsdam where he teaches international and German constitutional law and works on his PhD thesis on cyber security issues. Previously, he worked as a research assistant at the Walther-Schücking-Institute for International Law in Kiel, Germany.

Prof. Dr Thilo Marauhn is Professor of Public Law, International and European Law at Justus Liebig University, Giessen, Germany. He also is a permanent Visiting Professor of Constitutional Theory at the University of Lucerne. Thilo Marauhn is a member of the Advisory Board on United Nations Issues of the German Federal Foreign Office, a member of the German National Advisory Committee on International Humanitarian Law and a member of the International Humanitarian Fact-Finding Commission. He has published widely on the law of international security and, among other functions, is a member of the editorial board of the Journal of Conflict and Security Law (Oxford University Press).

Markus Maybaum is a German Air Force officer with more than 20 years of professional experience in the field of IT and IT security. Before his current assignment as a scientist at the NATO CCD COE's Research and Development Branch he worked in several different national and international management, leadership and expert positions focussing on information technology, software engineering, cyber security and arms control. Besides a diploma in business administration from the German Air Force College, Markus has a master's degree in informatics from the German Open University of Hagen, specializing in IT security. He is currently pursuing a PhD in information technology with a focus on technical aspects of arms control in cyber space at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Germany.

Dr Martha Mejía-Kaiser was born in Mexico City in 1957 and lives in Germany since 1989. She received a Licenciate's degree in International Relations, a Master's degree in International Law and a Doctorate in Political and Social Sciences from the National Autonomous University of Mexico (UNAM). She holds a Diploma in Air and Space Law from McGill University and is an International Space University graduate (89' Summer Session). She worked in the Mexican Foreign Affairs Ministry and the Geophysics Institute (UNAM). Dr Mejía has been acting as judge in the Manfred Lachs (Space Law) and Telders (International Law) Moot Court Competitions. Dr Mejía is invited lecturer at the International Institute of Air and Space Law, Leiden University (The Netherlands) and is Co-Chair of the Manfred Lachs Space Law Moot Court Committee, IISL. Dr. Mejía has published several articles and chapters in books on satellite remote sensing, space debris and the Geostationary Orbit.

Raimo Peterson is Chief of the Research & Development Branch at the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). Before his current assignment, he held diverse IT security management, leadership and expert positions for Siemens in Germany, South-Africa and Estonia. He has worked on large international IT security projects for the telecommunication industry and for the public sector. In his current position, Mr Peterson leads a group of researchers focusing on technical aspects of cyber defence, especially on monitoring, penetration testing, malware analysis and digital forensics. He holds a Diploma in Telecommunications from the Tallinn Technical University.

Mauno Pihelgas holds a Master of Science in Cyber Security from the joint master studies program of the Tallinn University of Technology and the University of Tartu. He also graduated from the Estonian Information Technology College in IT Systems Development. Coming from a mostly technical background, his previous professional experience includes a data center specialist and a monitoring specialist for Elion, a major Estonian IT and telecommunications company, which is part of the international TeliaSonera group. His current research at the NATO CCD COE (Technology / Research & Development Branch) focuses the field of cyber security, situational awareness and monitoring.

Dr Benedikt Pirker holds an LL.M. from the College of Europe in Bruges and a PhD from the Graduate Institute, Geneva, having also studied for a year at Sciences Po, Paris, and done a research visit at the University of Michigan Center for International and Comparative Law. He currently works as a post-doctoral researcher at the Institute for European Law at the University of Fribourg in Switzerland. His main research interests include public international law and European Union law, and more specifically international economic law and EU constitutional law.

Dinah PoKempner is general counsel of Human Rights Watch, one of the largest international human rights research and advocacy groups. Ms. PoKempner guides the organization in the development of its positions on international law and policy and directs its participation in litigation. She researches and writes on international humanitarian law, cyber-liberties, freedom of expression, religion and human rights, torture, and research ethics, among other topics. Ms. PoKempner's field work has taken her to Cambodia, the Republic of Korea, Vietnam, and the former Yugoslavia, and she has lectured and taught international law and human rights at many major universities and testified to the United States Congress on encryption policy. A graduate of Yale and Columbia University School of Law, she has also worked for the Office of the Legal Advisor of the United States Department of State.

Prof. Dr Michael N. Schmitt is the Charles H. Stockton Professor and Chairman of the International Law Department at the United States Naval War College. He is also Professor of Public International Law at the University of Exeter in the United Kingdom, a Senior Fellow of the NATO Cooperative Cyber Defence Centre of Excellence, and Editor-in-

Chief *of International Law Studies.* He has previously served as Dean of the George C. Marshall Center in Germany and General Editor of the *Yearbook of International Humanitarian Law.* Professor Schmitt is a retired United States Air Force officer, serves on many advisory and editorial boards, and is a Fellow of the Royal Society of Arts. From 2009-2013 he served as Director of the project leading to publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.

Heli Tiirmaa-Klaar held various managerial positions in the Estonian civil service from 1995. In 2007-2008 she led the inter-departmental working group that prepared the first Estonian Cybersecurity Strategy. In 2008-2010 she coordinated the implementation of the strategy, including the development of a new national critical information infrastructure protection system. She also worked closely with the European Union and NATO on cyber issues. In 2010-2011 she worked at NATO HQ, developing the current NATO Cyber Defence Policy. Since 2012 she works for the European External Action Service coordinating international cyber policy issues.

Prof. Joel P. Trachtman is Professor of International Law at The Fletcher School of Law and Diplomacy. Recent books include *The Future of International Law: Global Government,* Cambridge 2013; *The International Law of Economic Migration: Toward the Fourth Freedom*, Upjohn Institute 2009; *Ruling the World: Constitutionalism, International Law, and Global Governance*, Cambridge University Press 2009; *Developing Countries in the WTO Legal System*, Oxford University Press 2009; and *The Economic Structure of International Law*, Harvard University Press 2008. He has consulted for the United Nations, the OECD, APEC, the World Bank, the Organization of American States, and the U.S. Agency for International Development. Prof. Trachtman has served as a member of the Boards of the *American Journal of International Law*, the *European Journal of International Law*, the *Journal of International Economic Law*, the *Cambridge Review of International Affairs*, and the *Singapore Yearbook of International Law.* From 1998 to 2001, he was Academic Dean of the Fletcher School, and during 2000 and 2001, he served as Dean ad interim. He has been a visiting professor at Basel, Hamburg, Harvard, and Hong Kong. He graduated in 1980 from Harvard Law School, where he served as editor in chief of the *Harvard International Law Journal*.

Prof. Dr Ian Walden is Professor of Information and Communications Law and head of the Institute of Computer and Communications Law in the Centre for Commercial Law Studies, Queen Mary, University of London. His publications include *EDI and the Law* (1989), *Information Technology and the Law* (1990), *EDI Audit and Control* (1993), *Cross-border Electronic Banking* (2nd ed., 2000), *Telecommunications Law Handbook* (1997), *E-Commerce Law and Practice in Europe* (2001), *Computer Crimes and Digital Investigations* (2007), *Media Law and Practice* (2009), *Telecommunications Law and Regulation* (4th ed., 2012) and *Free and Open Source Software* (forthcoming, 2013). Ian has been involved in law reform projects for the World Bank, the European Commission, UNCTAD, ITU, UNECE and the EBRD, as well as for a number of individual states. Ian

was awarded a Council of Europe Human Rights Fellowship (1987-88); was a seconded national expert to the European Commission DG-Industry (1995-96); Board Member and Trustee of the Internet Watch Foundation (2004-09); on the Executive Board of the UK Council for Child Internet Safety (2010-12) and is currently a member of the Press Complaints Commission. Ian is a solicitor and Of Counsel to Baker & McKenzie. Ian leads Queen Mary's qLegal initiative, which is part of the iLINC network (http://www.qmul.ac.uk/qlegal/) and is a member of the Cloud Legal Project (http://www.cloudlegal.ccls.qmul.ac.uk/).

Dr Katharina Ziolkowski is legal advisor to the German Armed Forces, currently serving at the NATO CCD COE. Since she joined the legal service, Dr Ziolkowski served as the legal advisor to the project 'InfoOp and CNO Capabilities', as legal advisor and military prosecutor for the Airborne Operations Division of the German Armed Forces, and as legal advisor and law lecturer at the NATO School, the US Army's JAG School and the German General Command and Staff College. Dr Ziolkowski studied law and political science in Berlin and Barcelona and is admitted to the German bar. She holds a law degree from Freie Universität Berlin, an LL.M. in International Law from the University of New South Wales (Sydney) and a *magna cum laude* doctorate from Freie Universität Berlin, awarded by the Friedrich-Naumann-Foundation and the German Society for Military Law and the Law of War. Her research and writings focus on international law and international relations aspects of cyberspace.

Stability and security in international relations are preconditioned by predictability of State behaviour. Cyberspace is a rather new domain for State activities, and uncertainty with regard to international law, contemporary concepts of international relations and diplomatic agendas that apply to this arena during peacetime is commonplace. By offering a broad overview of the relevant topics and proposing interpretive approaches, this volume aims to bring increased clarity to this complex and important subject.

To assist the reader's orientation in cyberspace, the *first* part of this volume describes, in a comprehensive but accessible way, the sociological features and technical aspects of the internet and cyberspace. It explains the activities of State actors and their proxies, technical methods for remaining anonymous online and for back-tracing hackers, common cyber defence methods, techniques and tools, and the stages of hacking computer networks. The *second* part offers an interpretation of public international law with regard to rights and obligations of States in the cyber realm. The topics covered range from the notion of territorial sovereignty in cyberspace through international aviation, space and economic law restrictions to matters of responsibility of States and international organisations for cyber activities. The *third* part of the book elaborates on the interaction of States in cyberspace and governments' means of counteracting malicious cyber activities. The agenda and challenges of cyber diplomacy, a due diligence standard for cyber security, the means of economic and political 'cybered' coercion, and legal remedies are presented.

The authors of the book are renowned experts selected from a wide range of backgrounds, including academia, supranational and international organisations, governmental and non-governmental entities, the civilian as well as the military sector. Together, they have created a work which is the first of its kind and will constitute a benchmark in the field for many years to come.

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

ISBN 978-9949-9211-1-9
9 789949 921119