BENCH MEMORANDUM FOR JUDGES

THE CASE CONCERNING THE FROST FILES

Version 3.0

15 March 2016

CONFIDENTIAL

Only for use by Appointed Judges of the

2016 Philip C. Jessup Competition

Important Information regarding the Bench Memorandum

- The Bench Memorandum is a **confidential document** and should be read only by judges and administrators of the Jessup Competition. Every possible measure must be taken in order to maintain the confidentiality of the Bench Memorandum, including compliance with the following guidelines:
    - Do not leave copies of the Bench Memorandum lying in public places.
    - Do not, in any circumstance, discuss the Bench Memorandum or its contents with anyone else besides other Judges.
    - Do not, in any circumstance, distribute the Bench Memorandum to team members or team advisors, not even after the regional or national competition you have judged is over.
- If you have received this Bench Memo, you are no longer eligible to assist a team in any manner, including as a judge for practice oral rounds. **Doing so could result in the disqualification of the team from the competition**. See Official Rule 2.14.
- The contents of the Bench Memorandum will remain confidential until the conclusion of the International Rounds on April 2, 2016.
- The Bench Memorandum is copyright protected. Any entity that is not affiliated with ILSA or the Jessup Competition must request permission to use or reproduce any portion of the Bench Memorandum by emailing jessup@ilsa.org.
- The Bench Memorandum is an evolving document. As the competition season progresses, new versions of the Bench Memorandum will become available. ILSA encourages judges and competition staff to make sure they possess the most recent version of the Bench Memorandum.

ILSA welcomes comments and recommendations on the Bench Memo. Please send all suggestions to jessup@ilsa.org.

Table of Contents

PART 1: INTRODUCTION

I. PURPOSE OF THE BENCH MEMORANDUM

The Bench Memorandum provides judges with basic factual and legal information to evaluate the written and oral performances of participating teams. This Bench Memorandum should be read in conjunction with the 2016 Jessup Problem (the "*Compromis*") and the Corrections and Clarifications to the *Compromis*.

The *Compromis* was designed to present the competitors with a balanced problem such that each side has both strengths and weaknesses. Jessup teams should be able to construct logical arguments as both the Applicant and the Respondent. As a judge, your task is to evaluate the quality of each team's analysis, their knowledge of international law, and their advocacy skills. Please make sure not to confuse this task with your own personal evaluation of the merits of the case.

This document is not meant to be an exhaustive treatise on the legal issues raised in the *Compromis*. Judges should be aware that this document has been condensed in favor of breadth. It does not purport to cover every last detail, though we do aim to contextualize the law both within society and the events of the *Compromis*. In many instances, relevant case law and state practice is alluded to, but not discussed in depth. The participants should address these cases and principles of law. The state practice and legal authorities cited herein are illustrative and not intended to be a comprehensive review of all relevant sources of law. As such, judges should not be surprised when participants present arguments or cite authorities that may not be discussed in this memorandum. This does not suggest that such arguments are not relevant or credible.

This year's problem, in particular, raises numerous areas of legal discussion that involve ongoing debate and political controversy. Both in the context of the law surrounding espionage and electronic surveillance, and the law surrounding cyber activity, the emerging nature of technology and the cloak of secrecy draped around relevant practice, will play a significant role in the students' argumentation. Many teams may rely on emerging norms or on recent state practice, while others might turn to creative legal claims derived from both evolving customary rules and various general principles of international law. As a result, we anticipate greater diversity among teams' memorials and oral arguments than in previous years. Judges should provide students the necessary room to test out potential lines of reason, while maintaining a critical eye in evaluating the persuasive value of presented arguments.

As always, judges are encouraged to engage in their own independent research on the issues or examine the suggested research materials given to students. These materials are available online at www.ilsa.org: First Batch of Basic Materials (published 1 October 2015); Second Batch of Basic Materials (published 10 December 2015); Jessup *Compromis* Expert Panel Discussion (International Law Weekend, Fordham Law School, 7 November 2015).

II. SUMMARY OF THE CASE

This year's Jessup problem focuses on the growing tension between national security and civil liberties in combatting terrorism. Among the many issues raised in this year's *Compromis* are the legality of peacetime espionage and mass electronic surveillance, the subsequent seizure of equipment used to conduct said surveillance and the arrest of alleged spies, administrative detention and due process under international human rights law, and the attribution and legality of state sponsored cyber attacks.

The Applicant State, Amestonia, and the Respondent State, Riesland, are neighboring countries with historically friendly relations. Amestonia is a developing nation whose principal export is agricultural produce. Riesland is a developed constitutional-democracy with a rapidly expanding information and communications sector.

On 4 March 1992, the two countries signed the "Broadcasting Treaty," pursuant to which each state was permitted to build, staff, and operate a television station in the other's territory. In accordance with the Treaty, the Voice of Riesland (VoR), a division of the State-owned Riesland National Television, began broadcasting in Amestonia on 22 December 1992.

On 2 July 2013, a new website www.longlivethehive.com was launched, where environmental activists from both Amestonia and Riesland were congregating to discuss ways to stop the continued production and use of neonicotinoids (also known as "neonics"). This class of insecticide, produced solely by Rieslandic companies and used by Amestonian farmers to boost yields, was suspected of causing the collapse of bee and other pollinator populations across the region. The website, which provided anonymity on its online forum, was used by some activists to argue for violence.

On 2 February 2014 seven Amestonian warehouses containing barrels of neonicotinoids were torched, killing five people, including two Rieslandic nationals, and causing $75 million in damage. On 7 March 2014, 263 envelopes containing white powder, later discovered to be a non-toxic variant of neonicotinoid, were sent to the Ministries of Trade and Agriculture in both Riesland and Amestonia, to prominent Amestonian farmers, and to board members of three neonic-producing Rieslandic corporations. The Prime Minister of Riesland, Alice Silk, ordered its intelligence services to direct their operations against what she called the threat of "eco-terrorism".

Among these Rieslandic intelligence services is the Secret Surveillance Bureau ("the Bureau"), which mounts covert operations and collects secret intelligence outside of Riesland pursuant to the provisions of the Secret Surveillance Bureau Act (SSBA) of 1967. The Bureau is authorized to commit electronic surveillance and to acquire intelligence with the aim of aiding Riesland's ability to protect itself against national security threats and to conduct its foreign affairs. The Bureau's activities are subject to structural safeguards and minimization procedures under the SSBA. On the basis of a 1970 intelligence sharing arrangement, and in light of the growing terrorist threat, Bureau officials provided intelligence to their Amestonian counterparts. In one occasion, a plot to contaminate to contaminate a large shipment of honey intended for Riesland, was thwarted due to an early warning provided by the Bureau regarding a ring of environmental activists calling themselves "The Hive."

Frederico Frost, a Rieslandic national and a Bureau analyst, downloaded 100,000 top-secret documents and with the assistance of Chester & Walsingham, a law firm and *The Ames Post*, leaked the documents online between January and February of 2015. The documents revealed the nature and scope of two programs launched by the Bureau. The first, code-named Verismo, launched in May of 2013,

involved the installation of a recording pod on the undersea fiber optic cable that served the primary backbone of Amestonia's international internet and telephone communications traffic. 1.2 million gigabytes of data were collected and stored daily pursuant to Verismo. A second program, code-named Carmen, involved the VoR station. Since its inception, high ranking Amestonian public officials who were interviewed by VoR's top news anchor, Margaret Mayer, had their electronic devices hacked using a rootkit malware called "Blaster." In total, over a 100 Amestonian politicians, businessmen, and diplomats were routinely surveilled under this program.

On 16 February 2015 an Amestonian judge swiftly granted an emergency warrant, allowing Amestonian police to enter the VoR station and seize all equipment and property pending criminal investigation. Upon execution of the warrant, they found the station unattended save for TV broadcasting equipment, airing reruns of Mayer's show. That same night, members of the Amestonian Border Patrol detained Mayer and two other VoR employees while they were attempting to cross the border back into Riesland. Warrants were soon issued for their arrest and all are currently being held for the crime of espionage.

On 7 March 2015, Joseph Kafker, a retired Amestonian politician and a noted supporter of a ban on neonicotinoids, was arrested upon delivering the keynote address at a conference in one of Riesland's biggest law schools. He was soon detained under Riesland's Terrorism Act, in accordance with a terrorism alert declared in October 2014. Shortly thereafter, Kafker stood before the National Security Tribunal for closed proceedings. The Tribunal ruled that all information about Kafker's activities were "closed materials" and extended Kafker's detention for national security reasons. His lawyer, selected from a predetermined list of special advocates, was statutorily barred from disclosing or discussing any of the incriminating "closed materials" with Kafker. Kafker remains detained without charge in a maximum-security facility in Riesland and the Tribunal has extended his detention every 21 days.

On 14 March 2015, President of Amestonia, Jonathan Hale, instructed his Minister of Justice to refuse Riesland's request for the extradition of Frost and for the return of the documents he illicitly obtained. On 22 March 2015, and following yet another leak on *The Ames Post* website, the computer networks and switches at the *Post* and Chester & Walsingham were hacked to the extent that 90% of the information was "non-recoverable." Experts at the Amestonian Institute of Technology traced the hacking to IP addresses associated with Rieslandic governmental infrastructures. They further identified that significant segments of the malware used in the attack were an exact replica of the Bureau's "Blaster" program.

On 6 April 2015, and at the request of Amestonian government, divers from the German company that owned the undersea fiber cable identified the Verismo recording pod and dismantled it. On 22 April 2015, it was reported that Amestonia's Ministry of Justice applied for and obtained a forfeiture order for all of VoR's property. The Ministry is intending to sell the station's real estate and property, estimated to be worth €20 million, by public auction. In July 2015, Amestonia circulated among the members of the United Nations Human Rights Council the text of a proposed resolution calling on the Special Rapporteur on the Right to Privacy to investigate Riesland's cyber and surveillance programs' overall compliance with international law. Riesland's supporters on the Council, however, urged an immediate settlement of disputes. Growing public and international pressure has led, ultimately, to this case before the International Court of Justice.

PART 2: LEGAL ANALYSIS

I. THE ADMISSIBILITY OF LEAKED DOCUMENTS AND THE LEGALITY OF PEACETIME ESPIONAGE AND MASS ELECTRONIC SURVEILLANCE

QP1 asks the teams to first present arguments on the admissibility of evidence derived from Frost's leaked documents subsequently published in *The Ames Post*. They will then have to address the legality of the two intelligence collection programs launched by the Bureau and made public by *The Post*: The Verismo Program (mass electronic surveillance from an undersea communications cable); and The Carmen Program (targeted surveillance of over a hundred Amestonian public figures).

To fully examine these issues students may turn to an array of potential legal arguments, all of which hold some merit. ***Judges are encouraged to provide students with the space to flexibly experiment with these alternative arguments.*** *Furthermore given the complexity of the surveillance issues,* ***judges are advised to limit the discussion on admissibility to what is strictly necessary, so to quickly turn to the substantive legal issues surrounding QP1.***

Amestonia's Prayer for Relief	Riesland's Prayer for Relief
The documents published on the website of The Ames Post are admissible as evidence before the Court under the Court's liberal evidentiary regime; Riesland's Verismo and Carmen surveillance programs against Amestonian public figures and nationals violated the U.N. Charter principles of territorial integrity and non-intervention, the Right to Privacy as enshrined in the ICCPR, customary law of the sea, diplomatic and consular law, and generally constituted an abuse of rights.	The illicitly obtained documents published on the website of The Ames Post are inadmissible before the Court. There is no prohibition on peacetime espionage and Riesland's surveillance programs complied with its obligations under the U.N. Charter, the ICCPR, and customary diplomatic and consular law, and the law of the sea. Riesland had a right, and a duty, to collect intelligence to counter terrorism and Amestonia acquiesced to Riesland's surveillance practices.
Amestonia is thus entitled to an order directing the immediate cessation of those programs with assurances of non-repetition	The Court has no authority to order cessation of those programs with assurances of non-repetition.

A. The Admissibility of the Leaked Documents

1. The ICJ's Liberal Evidentiary Regime

Article 48 of the ICJ statute, which was copied *in verbatim* from the PCIJ's statute, provides that the Court shall "make all arrangements connected with the taking of evidence." In the practice of both the PCIJ and ICJ evidence "is seldom excluded,"[1] applying a broad and liberal evidentiary standard

[1] Neil H. Alford Jr., *Fact Finding by the World Court*, 4 VILL. L. REV. 37, 81 (1958); *See also* MANLEY O. HUDSON, THE PERMANENT COURT OF INTERNATIONAL JUSTICE, 1920-1945: A TREATISE, §520, at 571 (1943) ("The occasions have been rare in which the [PCIJ] has excluded evidence proffered, and no general rules for exclusion have been formulated");

whereby the parties "are largely free to present the evidence they consider necessary and timely."[2] That is not to say, however, that there are no barriers to the admission of evidence,[3] and Riesland will attempt to raise those before the Court.

2. Ex Injuria Jus Non Oritur and The Fruit of the Poisonous Tree Doctrine

Riesland may try to argue that "law does not arise from injustice," (*ex injuria jus non oritur*) and, as such, the documents, which were stolen by Frost and violated Riesland's domestic laws, should not be permitted to form the factual basis for a judgment by a court of law. Amestonia may counter by saying that "law arises from the facts" (*ex factis jus oritur*)[4] and that given that Amestonia is not the wrongdoer, but a third party, it should be allowed to present facts as reflected in those documents.[5] Riesland might counter by claiming that Amestonia's failure to timely seize the documents and extradite Frost makes it complicit in the wrongdoing and potentially even responsible for it.[6] Alternatively, Riesland may claim that "property obtained by crime is vitiated" (*crimen omnia ex se nata vitiat*), a doctrine which is known in U.S. practice as the exclusionary rule of "fruit of the poisonous tree." However, Amestonia may argue that this principle is unique to common law systems and that it is not uniformly applied even within these systems.[7] It has thus not reached customary level. For example, in the *Corfu Channel* case, while recognizing that the minesweeping operation conducted by the UK violated Albanian sovereignty over its territorial waters, the ICJ nevertheless accepted into evidence the information the UK submitted concerning those mines and relied on those facts in its judgment.[8]

3. Confidential Materials and Public Knowledge

In line with the U.S. arguments following the Snowden revelations, Riesland may try to argue that the documents that have been published have already caused irreparable harms to its national security by jeopardizing intelligence sources and exposing sensitive intelligence collection practices. Riesland would thus argue that, by admitting the documents into evidence, the Court would legitimize

---

DURWARD V. SANDIFER, EVIDENCE BEFORE INTERNATIONAL TRIBUNALS, 189-190 (1975) ("in practice... tribunals have been unwilling to exclude evidence in reliance upon general rules or principles.").

[2] The Swiss Memorial in the Interhandel Case, (Switz. v. U.S.) (Mémoire du Gouvernement de la Confédération Suisse, 1959 ICJ Pleadings 79, 128 (Memorial dated March 3, 1958)); *See also*, Eduardo Valencia-Ospina, Evidence Before the International Court of Justice, 1 Int'l L.F. D. 202, 204-205 (1999).

[3] For a discussion of such restrictions *see* W. Michael Reisman & Eric E. Freedman, *The Plaintiff's Dilemma: Illegally Obtained Evidence and Admissibility in International Adjudication*, 76 AM. J. INT'L L. 737, 741-745 (1982).

[4] Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, 2010 I.C.J. 141 ¶¶ 136–37 (Cançado Trindade, J., separate opinion).

[5] William Thomas Worster, *The Effects of Leaked Information on the Rules of International Law*, 28 AM. U. INT'L L. REV. 444, 447-449 (2013).

[6] Certain teams may argue that the decision not to extradite Frost on the basis of the "political offence" exception provided in the extradition treaty, which effectively granted Frost asylum in Amestonia, might constitute an act of "acknowledgement and adoption" as the term is defined under Article 11 of the ILC Articles on State Responsibility. This will allow Riesland to attribute Frost's actions to Amestonia, further justifying an *ex injuria* argument.

[7] Worster, *supra* note 5, at 455-466.

[8] Corfu Channel, (U.K. /Alb.), 1949 I.C.J. 4 (Apr. 9).

the stealing of confidential materials and reward whistleblowing, indirectly incentivizing further leaks. Riesland may draw parallels to the IBA Rules on the Taking of Evidence in International Arbitration, which many consider as reflective of best practices.[9] Rule 9(2)(f) establishes that an arbitral tribunal may exclude a document from evidence on "grounds of special political or institutional sensitivity (including evidence that has been classified as secret by a government [...])."[10] Amestonian advocates would benefit from clarifying that they do not seek to admit into evidence all of the 100,000 documents stolen by Frost but only those documents that already have been published by *The Ames Post*. Indeed, the ICJ in the *Tehran Hostages* case was willing to rely on "matters of public knowledge which have received extensive coverage in the world press"[11] as the basis of factual evidence. Relying only on the published materials thus dilutes any significant concern of further immediate harms to Riesland's national security or to the integrity of the Court.

4. Authenticity of the Documents

The practice of numerous international courts in relation to the admissibility of WikiLeaks documents, as summarized by the Special Tribunal For Lebanon,[12] involves an analysis of whether the documents are *prima facie* reliable, authentic and of probative value. Amestonia must assert a "high degree of credibility"[13] and establish whether "a document is what it professes to be in origin and authorship."[14] While Riesland has never acknowledged the documents to be authentic, it would benefit from conceding on this issue. The fact that divers were able to identify the recording pod based on coordinates provided in the documents, the level of detail of each of the documents in question, the fact that Riesland is requesting Frost's extradition for theft and data security offenses, and the process of authentication conducted by the *Post* itself, all *inter alia*, establish the necessary *indicia* of credibility. Note that "definitive proof of reliability and authenticity are not required at the admissibility stage."[15]

B. The Legality of Riesland's Surveillance Programs

1. The Lotus Doctrine and the Law surrounding Peacetime Espionage

The PCIJ in the *S.S. Lotus* case set the principle that in the absence of an explicit prohibitory rule, states remain free to act as they deem most suitable in the international sphere.[16] Many, if not most,

---

[9] PETER ASHFORD, THE IBA RULES ON THE TAKING OF EVIDENCE IN INTERNATIONAL ARBITRATION: A GUIDE, 6 (2013) (calling the rules a "useful harmonization of the procedures commonly used in international arbitration" and a direct result of the Arbitration Committee's desire to reflect "new developments and best practices in International Arbitration since 1999").

[10] *Rules on the Taking of Evidence in International Arbitration*, International Bar Association, Art. 9(2)(f) (29 May 2010).

[11] United States Diplomatic and Consular Staff in Tehran (United States v. Iran) 1980 I.C.J. Rep. 9.

[12] Prosecutor v. Salim Jamil Ayyash et. al., Decision on the Admissibility of Documents Published on the Wikileaks Website, Case No. STL-11-01/T/TC (21 May 2015).

[13] ConocoPhillips Petrozuata BV, ConocoPhillips Hamaca BV and ConocoPhillips Gulf of Paria BV v Bolivarian Republic of Venezuela, ICSID Case No ARB/07/30, Decision on Respondent's Request for Reconsideration, Dissenting Opinion of Georges Abi-Saab, ¶ 64 (10 March 2014).

[14] Rome Statute of the International Criminal Court, Art. 69(7), July 17, 1998, 2187 U.N.T.S. 90.

[15] Prosecutor v. Salim, STL Decision, *supra* note 12, at ¶ 11.

[16] S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18-19 (Sept. 7).

international legal scholars share the position that espionage, as a legal field, is devoid of meaning, and that no prohibitions exist on peacetime spying or other peacetime surveillance activity.[17] Thus, Amestonia would have to identify and argue for certain prohibitions on spying within either currently existing treaty law or emerging customary international law. Riesland will alternatively argue that outside such a prohibition, peacetime espionage is, from a *Lotus* perspective, *non liquet*: it is not regulated and therefore not justiciable under international law.

a. Territorial Integrity, Non-Intervention, and Notions of Consent

The "general principle of exclusive sovereignty over national territory is firmly established in customary international law,"[18] and is closely linked to the U.N. Charter principles of sovereign equality and non-intervention.[19] Indeed, the traditional doctrinal view has been that intelligence gathering within the territorial confines of another state, lacking specific agreement to that effect, may constitute an unlawful intervention.[20] Amestonia's status as a developing country might further exacerbate the potential infringement of sovereign equality by conducting these acts.

In *Canadian Security Intelligence Act Re (F.C),* the Federal Court of Canada ruled that obtaining access to, installing any thing to, searching for, making copies of, or otherwise recording electronic data are *per se* intrusive acts which are "likely to breach the binding customary principles of territorial sovereign equality and non-intervention, by the comity of nations."[21] Amestonia may rely on this case to establish that the Verismo program, by installing a recording pod on one of its main international communications cables and copying and analyzing enormous amounts of Amestonian data daily, constituted a breach of its sovereignty. Amestonia may further claim that, despite receiving intelligence that had been derived from Verismo, it was never made aware of the nature, scope, and reach of that program and, therefore, could not be said to have provided Riesland with "valid consent" as the term is defined by the International Law Commission (ILC).[22] Regarding the Carmen program, Amestonia may reference Article 23 of the Broadcasting Treaty, which clarifies that VoR employees were specifically prohibited from interfering in the domestic affairs of Amestonia. By spying on public figures and interfering in Amestonia's foreign policy (such as in the context of spying on Amestonian diplomats to

---

[17] *See, e.g.*, W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 433, 433-434 (John Norton Moore et al. eds., 1st ed., 1990) ("No serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each"); Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, A/HRC/10/3, 9 (Feb. 4, 2009) ("no general norm exists in international law expressly prohibiting or limiting acts of intelligence gathering").

[18] JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE, 83 (1995).

[19] Charter of the United Nations, 3 Bevans 1153, Art. 2(1), 2(4), 2(7) (1945).

[20] Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 TEMP. L.Q. 365, 419 (1973).

[21] *Canadian Security Intelligence Act Re (F.C)*, SCRS-10-07, CF 301, ¶ 52 (2008).

[22] For further reading, *see* International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, U.N. Doc. A/CN.4/SER.A/2001/Add.1, 72-74 (2001).

possibly influence Amestonian votes in the UN General Assembly and Specialized Agencies) the program constituted coercive intervention.[23]

Riesland will counter by claiming that the principle of non-intervention has "failed to keep pace with the technological advancements that render traditional territorial limits irrelevant."[24] Germany, for instance, argued before the European Court of Human Rights (ECtHR) that modern forms of electronic surveillance were "not contrary to public international law because the monitoring of wireless telecommunications did not interfere with the territorial sovereignty of foreign States."[25] Riesland will claim that the practice of foreign electronic surveillance is widespread and, despite its sheer volume, the number of actual protests by States against this activity has been insignificant.[26] It will further argue that Amestonia is estopped from challenging the legality of the Verismo program, as it tacitly consented or acquiesced to Riesland's surveillance practices. On at least 50 occasions, Riesland shared confidential information derived from Verismo with Amestonian security officials, in accordance with the intelligence sharing arrangement between the two countries. Amestonia, thus, may be said to have known, or at least should have known, that its nationals were under surveillance. Spying on heads of State and public figures, as was done in the Carmen program, is a common and fairly accepted practice in international affairs.[27] All in all, Riesland will contend, the intelligence collected through these programs benefitted not only the national security of both countries, but also their joint economic prosperity (Amestonia's GDP growth through trade relations with Riesland being the evidence of that).

b. International Human Rights Law and the Right to Privacy

The right to privacy is a fundamental human right enshrined in the United Nations' Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), and in many other international and regional treaties.[28] Students will have to address, however, both the

---

[23] To coerce another State in order to obtain from it the subordination of the exercise of its sovereign free choice or to secure from it advantages of any kind is prohibited, *see* Declaration on the Inadmissibility of Intervention on the Domestic Affairs of States and the Protection of their Independence and Sovereignty, G.A. Res. 2131, U.N. GAOR, 20th Sess., Supp. No 14, Dec. 21, 1965; *Military and Paramilitary Activities in and Against Nicaragua* (*Nicar. V. U.S.*), Judgment 1986 I.C.J. 14, ¶ 205 (June 27).

[24] Simon Chesterman, *The Spy Who Came in From the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L. L. 1071, 1098 (2006).

[25] Weber & Saravia v. Germany, app no. 54934/00, Euro. Ct. Hum. Rts., ¶ 81 (2006).

[26] *See* McDougal, Lasswell & Reisman, *supra* note 20, at 394.

[27] Consider, *inter alia*, Australian surveillance of East Timorese businessmen and public figures during treaty negotiations; U.S. surveillance of the heads of State of Germany, Brazil, and Mexico, among others; NSA and GCHQ surveillance of all member missions of the Security Council in the lead up to the war on Iraq; or Canadian and Russian surveillance of all participants in the G20 summits which they hosted in 2010 and 2013 respectively.

[28] *See, e.g.*, Universal Declaration of Human Rights Article 12; International Covenant on Civil and Political Rights Article 17; Convention on the Rights of the Child, Article 16; Convention on the rights of Migrant Workers Article 14; The European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8; The African Charter on the Rights and Welfare of the Child, Article 10; The American Convention on Human Rights, Article 11; The Arab Charter on Human Rights, Article 21.

geographical and personal scope of protection (the extraterritorial reach of the ICCPR) as well as the particular substantive standards applied by courts in identifying unlawful interference with the right.[29]

Article 2 of the ICCPR requires each State party to respect and ensure to all persons within its territory and subject to its jurisdiction the rights recognized in the Covenant. This two-pronged test has led a number of prominent countries, such as the U.S. and Russia, to argue that the ICCPR does not impose obligations beyond the borders of the member States. Amestonia will rely, *inter alia*, on the jurisprudence of the ICJ in the *Wall Advisory Opinion*, as well as on the Human Rights Committee (HRC) practice as reflected in General Comment 31,[30] to establish that "a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking at home."[31] Amestonia will claim that both "foreigners" and "citizens" should have equal access to privacy protections. Riesland will contend that, even if it were to recognize the potential extraterritorial reach of the ICCPR, such reach is limited, as evidenced in the ECtHR's *Bankovic* decision, only to situations of effective control over a territory or person.[32] Copying data using an underwater recording pod (Verismo) or electronically hacking and accessing the devices of particular targets (Carmen) falls short of such a high standard of "authority and control".[33] Amestonia may challenge, claiming that the "interference" with the right took place at the moment data was stored in Rieslandic databases and analyzed by Bureau employees, over both of which Riesland had full jurisdiction. It may further argue that, similar to jurisdiction over an embassy, Riesland enjoyed full control over the territory of the VoR station from which the Carmen program was conducted. Amestonia can indeed point to UNGA Resolution 68/167,[34] as well as the practice of the HRC,[35] which recognize the ICCPR's applicability in such circumstances.

---

[29] Certain teams may argue that Amestonia lacks standing to raise ICCPR claims, as it cannot exercise diplomatic protection over all nationals as a mass claim before the Court. While it is true that the 2006 Draft Articles on Diplomatic Protection require identifiable injury to a national for invocating responsibility, it is sufficient to show in the context of a privacy violation only "reasonable likelihood that a person has been subjected to unlawful surveillance." The European Court of Human Rights clarified that "owing to the secrecy [of intelligence activity...], an individual may [...] claim to be the victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures, without having to allege that such measures were in fact applied to him." If this were not so, "the efficiency of the Convention's enforcement machinery would be materially weakened." Klass and Others v. Germany, Judgment, App. No. 5029/71, Eur. Ct. H.R., ¶ 34 (6 Sept. 1978). See also the approach of the Court in Roman Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H. R., ¶ 171, 178 (4 Dec., 2015).

[30] For an analysis of differing views on extraterritoriality in the applicability of the ICCPR *see* Marko Milanović, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56(1) HARV. INT'L. L. J. 81, 97-111 (2015).

[31] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37, ¶ 33 (June 30, 2014).

[32] Banković v. Belgium, Decision on Admissibility, App. No. 52207/99, Eur. Ct. H.R (December 12, 2001).

[33] For an analysis of the applicability of the ICCPR to extraterritorial surveillance see Milanović, *supra* note 30, at 120-130.

[34] United Nations General Assembly Resolution A/RES/68/167 (December 18, 2013) ("Noting that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern") (adopted without a vote).

Under Article 17 of the ICCPR Interference with an individual's right to privacy is permissible only if it is neither arbitrary nor unlawful. The HRC and regional human rights courts have set certain tests to determine the lawfulness of particular surveillance programs. Each program must be authorized by laws that (a) are publicly accessible and foreseeable; (b) contain provisions that ensure that collection of, access to, and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying the exact circumstances in which interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; (d) are proportional to the end sought, necessary in the circumstances of any given case, and be the least intrusive measure available; (e) provide for effective procedural safeguards against abuse, including effective, adequately resourced institutional arrangements; and (f) provide for effective remedies for violations of privacy.[36]

A number of recent cases from the ECtHR shed light on the substantive content of the right to privacy. In *Roman Zakhrov v. Russia* the ECtHR delivered a particularly relevant judgment where it found serious and systematic faults with the Russian legislative framework regulating the surveillance of mobile communications. The Court took a variety of elements into account including, *inter alia*, the breadth of discretion granted to the executive in determining what constitutes national, economic, and ecological security; the fact that interception authorizations were sometimes granted in bulk and not against a specific target; and the fact that the government was unable to provide the Court with any examples of effective oversight.[37]

Similarly in *Szabó and Vissy v. Hungary*, the ECtHR reiterated its previous position in *Digital Rights Ireland v. Minister for Communications* that secret surveillance must correspond to the criteria of being "strictly necessary" for the safeguarding of democratic institutions or for the obtaining of vital intelligence in an individual operation.[38] Furthermore, the Court redefined the scope of States' margin of appreciation in choosing surveillance measures, noting that when balancing a state's national security interest in utilizing "secret surveillance measures" against the "seriousness of the interference" in privacy, a state has a certain "margin of appreciation" in choosing its means to achieve this "legitimate aim of protecting national security." However, this margin is subject to "European supervision [including] both legislation and decisions applying [said legislation]." The ECtHR further opined that the risk of secret surveillance undermining the very democracy it sought to defend, required to the Court to be "satisfied that there are adequate and effective guarantees against abuse."[39]

Amestonia and Riesland will argue in favour or against the existence of these standards in the context of the both the overarching SSBA and the specific Verismo and Carmen programs. The facts were drafted in such a way to be balanced on this point. While the SSBA is publicly accessible, the

---

[35] *See, e.g.*, Human Rights Committee, Concluding Observations on the Fourth Report of the United States of America, ¶ 22 (March 28, 2014), *available at* https://goo.gl/vUNxdZ.

[36] For a summary of these standards and the jurisprudence of the HRC and ECtHR from which they were derived *see* Report of the U.N. OHCHR, *supra* note 31, at ¶ 21-41.

[37] *See*, Zakharov v. Russia, *supra* note 29, at ¶¶ 248, 265, 284.

[38] Szabó and Vissy v. Hungary, App. No. 37138/14, Eur. Ct. H. R., ¶ 73, 178 (12 Jan., 2016).

[39] *Id.*, at ¶ 57.

specifics surrounding the two programs were secret. Though legitimate aims are indeed defined within the SSBA, they may be too broad and over-encompassing, effectively authorizing unfettered surveillance. Further, while there exists a mixed institutional model of parliamentary and judicial oversight, these were potentially inadequate in ensuring accountability and Riesland might be unable to show effective oversight. Students will also benefit from distinguishing between the Verismo and Carmen programs: the former is a classic mass surveillance program while the latter is targeted against specific public figures (who themselves might have lower expectations of privacy). Applying necessity, proportionality, and reasonableness in both cases, might produce different legal and factual results in terms of the actual level of intrusiveness as well as the overall infringement on the right to privacy.

c. International Counter-Terrorism Law and Abuse of Rights

Riesland will argue that the right (if not the obligation) to collect intelligence to fend off terrorist activity is a derivative of its inherent right of self-defense,[40] a reflection of Security Council Chapter VII binding resolutions,[41] and a requisite of treaty law to which both States are parties.[42] Riesland can either use these sources to set the background on the legality of its overall intelligence activity, or as a separate unique U.N. Charter Article 103 argument (whereby its ICCPR obligations, to the extent that they conflict with its Charter obligations to collect intelligence, are bypassed with the latter prevailing). Amestonia may try to counter the specific Article 103 argument by referencing the European Court of Justice's *Kadi* ruling.[43] More generally, it may argue that while Riesland may enjoy a right to collect intelligence, such a right may not be used to impede the enjoyment of other States of their own rights, or for an end different from that for which the right was created, as these would constitute an abuse of rights. Thus, Amestonia will claim that by violating its territorial integrity, and by collecting intelligence not only for national security reasons but also for broader economic and foreign policy interests, Riesland abused its Charter rights.[44]

d. Law of the Sea and the Verismo Program

The Verismo program involved the installation of a waterproof recording pod on the undersea fiber optic cable, which acted as the primary backbone for Amestonia's international communications traffic. The device was placed on a section of the cable located in Riesland's Exclusive Economic Zone

---

[40] U.N. Charter, *supra* note 19, Article 51.

[41] *See, e.*g., U.N. Security Council Resolution 1373, S/RES/1373 (2001) (regarding certain obligations to intensify and accelerate the exchange of operational information to prevent the commission of terrorist acts. Note, however that the resolution clarifies that any such exchange must be done in accordance with international law).

[42] *See, e.g.*, U.N. Convention for the Suppression of Terrorist Bombings, 2149 UNTS 256, Article 15 (1997); International Convention for the Suppression of the Financing of Terrorism, 2178 U.N.T.S. 197, Article 18 (1999) (setting obligations upon member States to collect and exchange information to prevent terrorist activity).

[43] Joined Cases C-402 & 415/05P, Kadi & Al Barakaat Int'l Found. v. Council & Comm'n, 2008 E.C.R I-6351 (2008) (whereby the European Court of Justice recognized that fundamental human rights guarantees could not be superseded by the U.N. Charter or Security Council Resolutions. Note, however that the Court established its claim on the basis that EU law constituted an "internal" and "autonomous" legal system existing on a separate plane from the U.N. Charter).

[44] On the issue of abuse of rights and international law, *see* G.D.S. Taylor, *The Content of the Rule against Abuse of Rights in International Law*, 36 BRIT. Y.B. INT'L L. 323 (1972).

(EEZ). Although neither country is party to the U.N. Convention on the Law of the Sea, Amestonia may recall the law surrounding the EEZ regime, which has been recognized by the ICJ as reflective of customary international law.[45] Amestonia will argue that by placing the pod, Riesland (as the coastal State) violated its obligations to have "due regard" to the rights of other States,[46] as well as to exploit its EEZ only within the ambit of "internationally lawful uses"[47] and for "peaceful purposes".[48] Riesland will counter by turning to vast state practice, from the U.S. Ivy Bells operation during the Cold War to the modern-day British Tempora program to demonstrate that the tapping of underwater cables for intelligence purposes is recognized as an internationally lawful activity serving peaceful purposes.[49] Furthermore, Riesland will argue that the pod did not cause any injury or damage to the cable, nor did it interrupt or obstruct communications.[50]

e. Diplomatic Law and the Carmen Program

The Carmen program involved, in part, the interception of communications of former and current diplomats, including Amestonia's ambassador to the U.N. In accordance with the Vienna Convention on Diplomatic Relations (VCDR), the person of the diplomat, the mission's premise, and diplomatic communications are inviolable.[51] "From that, one might argue that it is unlawful [for any State] to penetrate that mission, even using electronic means."[52] Similarly, spying on U.N. ambassadors is also in violation of Article 105(2) of the U.N. Charter.[53] Riesland will counter by referring, again, to the vast practice of States spying on diplomatic missions, including U.N. missions.[54]

---

[45] *Case Concerning the Continental Shelf (Tunis. v. Libya)*, 1982 I.C.J. 18, at para. 100 (Feb. 24).

[46] United Nations Convention on the Law of the Sea, Article 56(2), 1833 U.N.T.S 397 (1982).

[47] *Id.,* Article 58(1).

[48] *Id.,* Article 88.

[49] For further reading *see* Wolff Heintschel von Heinegg, *Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables Under International Law*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 291, 295-296 (Katharina Ziolkowski ed., 2013) .

[50] *Id.,* Article 113.

[51] Vienna Convention on Diplomatic Relations, 500 U.N.T.S. 95, Art. 22, 27, 29 (1961).

[52] Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 312 (2015).

[53] U.N. Charter, *supra* note 19, Article 105(2) ("Representatives of the Members of the United Nations and officials of the Organization shall similarly enjoy such privileges and immunities as are necessary for the independent exercise of their functions in connection with the Organization").

[54] At the time of the enactment of the Foreign Intelligence Surveillance Act in 1978, the issue of electronic surveillance of diplomatic premises and its compatibility with the rules of the Vienna Convention on Diplomatic Relations was discussed at length in Congress. As noted by Professor Forcese: "[t]he Administration overcame this concern by supplying a list of states that surveilled U.S diplomatic premises abroad, suggesting that such a widely accepted practice, while not authorized by the Convention, did not violate it." (Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT. SEC. L. & POL. 179, 197 (2011). *See also*, Deeks, *Id.,* at 312-313.

C. Remedies: Immediate Cessation with Assurances of Non Repetition

In accordance with Article 30 to the ILC Articles on State responsibility, a State is required to cease a wrongful act if its *continuing*, and to provide assurances of non-repetition in situations where the injury suffered is *substantive,* and the risk of repetition is *real*;[55] In the present case, Riesland might try to challenge both arguments. On the continuing nature, Riesland will contend that the pod has been dismantled and the VoR station is no longer in operation; therefore, both the Verismo and Carmen programs have ceased. On the other hand, Amestonia might argue that the Blaster is still installed on the devices of its targets and that Riesland is still in possession of enormous amounts of data collected through Verismo. Therefore, the wrongful act is *continuing*. With regards to assurances of non-repetition, Amestonia will argue that the risk of new surveillance programs by Riesland, who has not yet apologized for its actions, is significantly real. Riesland will contend that it is inappropriate to turn to this extreme measure. Even if the Court holds that all past intelligence activities by Riesland were unlawful, Riesland will assert that this holding cannot conclusively determine the legality of future intelligence collection programs whose legality would have to be examined separately on the basis of their individual merits.

[55] ILC Articles on State Responsibility, *supra* note 22, at 88-91.

II. THE BROADCASTING TREATY, IMMUNITIES, AND SEIZURE OF ASSETS

QP2 raises issues of treaty interpretation, treaty termination, immunities law, and States' property rights under international law. The backdrop for the analysis lies with Amestonia's criminal investigation into the alleged spying and surveillance activity that took place inside the premises of VoR. Students will have to analyze whether Amestonia violated international law by seizing both the station and its devices, and later arresting three of its employees for charges of espionage.

Amestonia's Prayer for Relief	Riesland's Prayer for Relief
The seizure and forfeiture of the VoR station and its equipment, and the arrest of Margaret Mayer and the other two VoR employees, did not violate the Broadcasting Treaty, which in any event Riesland may not invoke either because it was invalidated, terminated, or for its own unclean hands. Further, Riesland cannot claim state immunity or unjust enrichment as arguments against Amestonia's lawful conduct.	The arrest of Margaret Mayer and the two other VoR employees, and the expropriation of the VoR facility and its equipment, violated the Broadcasting Treaty (which is still in force). Amestonia may not invoke necessity to preclude its wrongfulness. Amestonia further violated Riesland's state immunity and should immediately release the three VoR employees as well as compensate Riesland for the value of the confiscated property which was unjustly seized.

A. The Broadcasting Treaty and Treaty Interpretation Arguments

1. The Parties Rights and Duties Under the Treaty

According to Article 14(1) of the Broadcasting Treaty (BT), the premises of the VoR station were inviolable, and every entry into the station by Amestonian agents required either the explicit consent of the head of the station (or her assumed consent) *inter alia* in cases of an immediate threat to public safety. Articles 14(2) and 14(3) affirm that, both the premises of the station, its equipment, and other property used in its operation were immune from search, requisition, attachment, expropriation, or execution. Further, Amestonia as the host State was required to ensure the peace of the premises and prevent any impairment to its dignity. Finally, Article 14(4) clarifies that all of the stations' marked documents and archives are to be inviolable at all times, wherever they may be.

Article 15(1) grants the Rieslandic employees of the VoR station immunities and privileges, including those from criminal jurisdiction, arrest and detention. Article 15(1)(c) further clarifies that with respect to acts performed by an employee in the exercise of the station's functions, the immunities and privileges shall continue to subsist even after the employee's functions have come to an end.

Article 23(1) clarifies that, without prejudice to said immunities and privileges, Rieslandic employees of the VoR station were not only required to respect the laws of Amestonia but were also prohibited from interfering in Amestonia's internal affairs. Article 23(2) adds that the VoR station's premises cannot be used in any manner incompatible with either the station's functions envisaged within the treaty or with other rules of international law.

Finally Article 36 notes that all privileges and immunities, as listed in Articles 14 and 15 (except those listed in Article 15(1)(c)), shall cease to have effect upon the "cessation of the station's functions as envisaged in the Treaty."

2. The Law on Treaty Interpretation

Article 31(1) of the Vienna Convention on the Law of Treaties (VCLT), which is recognized by the ICJ as reflective of customary international law,[56] provides that a treaty "shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[57]

Furthermore, in accordance with the maxim of "*lex specialis derogate legi generali*," the BT shall prevail over general diplomatic and consular law as enshrined in the Vienna Convention on Diplomatic Relations (VCDR), Vienna Convention on Consular Relations (VCCR), and the Special Missions Convention (SMC). Nonetheless, the wording of the BT is, in relevant parts, an exact replica of the wording of the VCDR, VCCR, and SMC. The ICJ has, in the past, interpreted a treaty by looking at other treaties with similar language.[58] In this regard, students may look to the VCDR, VCCR, and SMC, in cases of particular lacunas within the BT, as a way of complementing that inadequacy. On the other hand, students may not simply transplant wholesale into the BT missing clauses present in the VCDR, VCCR, and SMC.[59]

3. Semantic and Temporal issues Surrounding "cessation of the station's functions as envisaged in the present Treaty"

Amestonia will rely on Article 36 of the BT to establish that, at the time of the emergency warrant for seizure of VoR's assets and property, it was not bound to uphold any of the immunities or privileges. Article 36 establishes that once the station ceases its functions, all immunities and privileges cease with it. The station's functions are addressed in both subparagraph (c) of the BT's preamble and in Article 2, which speak about the production and airing of programs. The judge granted the warrant concurrent to the interruption in VoR's broadcasting and the airing of old reruns of "Tea Time with Margaret." The Amestonian police found the station unattended, and, thus, were unable to request permission from the head of the station to enforce the search warrant. In this regard, Amestonia would contend that it was entitled to enter the station, as Article 14(1) provides that consent to enter may be assumed in situations of immediate threat to public order (Amestonia will claim that the espionage conducted in the facility constituted such a threat). Overall, the combination of a complete abandonment

---

[56] Territorial Dispute (Libya/Chad), 1994 I.C.J. 6 ¶ 41; Kasikili/Sedudu Island (Botsw. v. Namib.) 1999 I.C.J. 1045 ¶ 18.

[57] Vienna Convention on the Law of Treaties, 1155 U.N.T.S. 331, Article 31(1) (1969).

[58] Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo), Merits, 2010 I.C.J. 639 ¶ 68 (The ICJ in its interpretation of the ICCPR, "took note" of the interpretation of the respective regional courts of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the American Convention on Human Rights (ACHR). When justifying this interpretive move, the ICJ pointed to the fact that the provisions in the ICCPR, ECHR, and ACHR are "close in substance").

[59] Certain teams may try to claim that the VoR station is itself a diplomatic, consular, or special mission; thereby calling for the application of the VCDR, VCCR, or SMC directly. The existence of a BT as a separate legal regime, drafted by the parties for that reason, prevents teams from effectively making such a claim.

of the station coupled with the airing of an old tape (which will inevitably run out) could be interpreted as a "cessation of functions," as the station effectively stopped producing and airing programs.

Riesland will challenge this analysis. It may first argue that, as a matter of time, the Amestonian police applied for an emergency warrant before the interruption in broadcasting making the application itself a violation of the BT. Furthermore, Riesland may claim that at all times the station continued to serve its function as content was still being aired when the police entered the VoR station and seized all of its equipment. Riesland can also argue that the very act of *The Ames Post* continuing to leak secret documents, despite Riesland's expressed concern over the inflammatory publications, constituted a violation of Amestonia's own duty to protect the VoR station under Article 14(2). This would, arguably justify the temporary abandonment of the station. Even, *assuming arguendo*, that the station ceased its functions, certain immunities should, nonetheless. continue to persist. In particular, Riesland may argue that the wording of Article 14(4), which clarifies that all documents and archives shall remain inviolable "at all times and wherever they may be," demonstrates that Amestonia was not allowed to seize those documents and servers.[60] Finally, Riesland may try to claim that, in line with Article 15(1)(c), Margaret Mayer and the two VoR employees could not have been arrested, as their immunities and privileges continued to subsist even if the station had ceased its functions. Amestonia may argue in response that any spying activities conducted by the three do not qualify as "acts performed in the exercise of the station's functions" and, therefore, do not fall within the ambit of subsisting immunities. Riesland will counter that there is no evidence in the case showing that the three were, in any way, directly involved in any spying activities.

Certain Amestonian teams may try to argue that the station ceased its functions upon launching its surveillance activities in 1992. These activities do not serve to foster friendly relations, which the preamble to the BT establishes as its object and purpose. Judges may challenge whether the object and purpose of the BT is akin to or, alternatively, overrides, the functions of the station. Clearly, the station's regular functions were to produce and air programs. Insofar as the VoR did that successfully (producing "award winning documentaries and highly-acclaimed programs" for well over 22 years), it would be difficult to show how its functions were not fulfilled during that time. Moreover, given that surveillance was conducted in the VoR station since its inception, any suggestion that the surveillance itself entailed a cessation of functions, would also result in a situation where the VoR facilities and its employees never enjoyed the immunities enumerated in the BT to begin with. Judges should challenge whether that is a good faith reading of Article 36 and, in any event, should direct students to argue "cessation of functions" in the context laid out above.

4. The Legal Regime of Persona Non Grata

The sanction of "persona non grata" is "long established in customary international law and is recognized as the primary deterrent against the abuse of diplomatic privileges and immunities."[61] It aims to strike a balance between principles of sovereignty and territorial jurisdiction on the one hand and the

---

[60] Note, however, the potential conflict between the wording of Article 14(4) and Article 36. The latter, doesn't recognize an exception for Article 14(4), like it does for Article 15(1)(c). Students raising Article 14(4) will have to resolve this glaring omission.

[61] J. CRAIG BARKER, INTERNATIONAL LAW AND INTERNATIONAL RELATIONS, 166 (2000).

principle of inviolability and immunity on the other hand.[62] When a person holding diplomatic immunity is identified as a spy, the long-standing practice of States has been to declare these agents as *persona non grata*, notify the sending State, and order their expulsion.[63] As the ICJ recognized in the *Tehran Hostages* case: "This is the power which every receiving State has, at its own discretion, to break off diplomatic relations with a sending State and to call for the immediate closure of the offending mission."[64] Although the BT is lacking a provision establishing *persona non grata*, Riesland will contend that Amestonia had the right and indeed the duty to expel the VoR employees either as a matter of customary international law, or by way of interpreting the BT in line with the *lex generalis* of the VCDR, VCCR and SMC. Amestonia will claim that the BT is the *Lex Specialis*, and that by not including a *persona non grata* clause, the parties were effectively signaling their intention to grant only limited immunities that under certain circumstances could be completely revoked. Immunities and privileges are provided, both within the BT and under customary international law, to ensure the effective performance of the tasks the state officials have been sent to perform on behalf of their state. Amestonia will contend that by transgressing from their agreed-upon functions, the VoR employees lost the ability to claim their immunities. Furthermore, the moment and nature of apprehension should also be taken into consideration. The three VoR employees were apprehended at the border between the two countries and only after they refused to identify or provide documentation establishing their status.

B. The Treaty's Force, Unclean Hands and The Doctrine of Necessity

1. Invalidity of Treaties

a. Fraud

Article 49 of the VCLT provides that: "If a State has been induced to conclude a treaty by the fraudulent conduct of another negotiating State, the State may invoke the fraud as invalidating its consent to be bound by the treaty."[65] By invalidating the treaty, Amestonia will be able to claim that it was never bound to provide any of the immunities or privileges. There appears to be no precedent to guide this inquiry other than the ongoing case between Australia and East Timor at the Permanent Court of Arbitration.[66] Amestonia might argue that Riesland misrepresented its intentions in negotiating the

---

[62] Marcel Hendrapati, *Legal Regime of Persona Non Grata and the Namru-2 Case*, 32 J. L. POL'Y & GLOBALIZATION 161, 165 (2014).

[63] For an historical review of the practice of States with regards to the initiation of proceedings against alleged spies, including former diplomats, *see* ELIZABETH HELEN FRANEY, IMMUNITY, INDIVIDUALS, AND INTERNATIONAL LAW: WHICH INDIVIDUALS ARE IMMUNE FROM THE JURISDICTION OF NATIONAL COURTS UNDER INTERNATIONAL LAW? (2009)

[64] Case Concerning United States Diplomatic and Consular Staff in Teheran (Judgment) (U.S. v. Iran) 1980 ICJ 3, ¶ 85 (1980).

[65] VCLT, *supra* note 57, at Article 49.

[66] In April 2013, East Timor launched arbitral proceedings against Australia in relation to a dispute arising from a 2006 bilateral maritime agreement. Australian intelligence bugged the cabinet room where treaty negotiations over gas extractions from the East Timor Sea were taking place. The details of the arbitration in the PCA have not been made public, however, one of the arguments raised by East Timor is that Australia's bad faith during treaty negotiations necessitates the invalidation of the treaty. If accepted, East Timor will be the first country to successfully invoke Article 49's Fraud provision. For further readings *see* Kate Mitchell & Dapo Akande, *Espionage & Good Faith in Treaty Negotiations: East Timor v. Australia*, EJIL: Talk! (20 January 2014), *available at http://goo.gl/isizPx*.

BT, as Riesland intended to use the premises for espionage all along as the station was in fact used for this purposes "since its inception." Riesland may counter, however, that Amestonia would need to show evidence of the elements of fraud during negotiations, which the ILC has defined as "false statements, misrepresentations, and other deceitful proceedings" aimed at inducing a state's consent.[67] Riesland can argue that no direct facts exist in the *Compromis* to suggest that Riesland misrepresented its aims during treaty negotiations or that Amestonia was in any meaningful way "induced" by any such misrepresentations.

2. *Termination of Treaties*

a. *Material Breach Since Treaty's Inception*

Inadimplenti non est adimplendum, codified in Article 60(1) of the VCLT,[68] is a customary principle of international law, [69] that justifies the termination of a bilateral treaty, or the suspension of its operation, in whole or in part, due to a material breach by one of the parties. As the ICJ held in the *Namibia* case, a breach is material if the breached provision is "essential to the accomplishment of the object and purpose of the treaty."[70] By engaging in spying activities from the VoR facility, Riesland breached both Articles 23(1) and 23(2) of the BT. As already alluded to, Amestonia will contend that the BT's preamble, alongside the statements made by ministers from both states at the signing ceremony, form the treaty's object and purpose ("fortifying friendship", "strengthening understanding and cooperation", "another milestone in what is already the warmest of friendship between our two societies"). This object and purpose makes its use as a means of spying antithetical to the function of the station. Amestonia will claim that by violating both Amestonian domestic law as well as international law, and by interfering in its internal affairs, Riesland materially breached the BT. If accepted, Amestonia will be able to claim that the treaty was terminated since "its inception," or at the very least from the moment it was made aware of the transgressions. In both scenarios, Amestonia would no longer be bound to uphold the immunities and privileges listed in the BT.

Riesland will challenge this analysis. Predominantly, Article 23's usage of the term "without prejudice" makes clear that the parties did not intend for breaches of the Article to justify the revocation of immunities and privileges. Indeed, any good faith reading of Article 23(1) would establish that the parties did not consider at the time the treaty was drafted that violations of the obligations enumerated in Article 23 would be severe or material enough to justify the termination of the treaty altogether. Furthermore, Riesland will also note that Amestonia did not meet the procedural requirements listed in Articles 65-67 of the VCLT.[71] Articles 65-67 require the State seeking termination to (1) give advanced

---

[67] International Law Commission, Final Draft, Commentary to Article 46, 244-245, para. 3, *reprinted in* VIENNA CONVENTION ON THE LAW OF TREATIES: A COMMENTARY 840 (Oliver Dörr & Kirsten Schmalenbach, eds., 2012).

[68] VCLT, *supra* note 57, at Article 60(1).

[69] Gabčikovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶¶ 46, 99 (1997); Charlton v. Kelly, 229 U.S. 447, 473 (1913) (U.S.); LORD MCNAIR, THE LAW OF TREATIES 570-71 (1986).

[70] 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 I.C.J. 16, ¶ 94 (1971).

[71] VCLT, *supra* note 57, at Art. 65-67.

written notice of its intention to unilaterally terminate; (2) seek peaceful settlement of the dispute if the other party objects within 90 days from moment of notification; and (3) submit the matter to dispute resolution if no solution is reached within a year.[72] None of these requirements were met.

3. Riesland's Invocation of the BT and Unclean Hands[73]

Amestonia can further argue that Riesland is barred from asserting rights under the BT by virtue of the clean hands doctrine. This doctrine presents a general rule of equity that a "person who asks for redress must do so with clean hands."[74] Amestonia can argue that Riesland's breaches, from the very inception of the station, had caused or provoked its own conduct. The seizure of the station and its equipment, along with the arrest of its three employees, were done for the purposes of a criminal investigation that directly responded to evidence of espionage at VoR. The PCIJ noted that a general principle exists "that one Party cannot avail himself of the fact that the other has not fulfilled some obligation or has not had recourse to some means of redress, if the former Party has, by some illegal act, prevented the latter from fulfilling the obligation in question."[75] If Riesland were to gain redress against Amestonia for violations of the BT's immunities provisions, when it was Riesland's own surveillance (arguably a long-standing breach of the same treaty) that triggered the Amestonian reaction, it would seem to be unjust as a matter of equity. Riesland can counter that, despite certain references by the PCIJ and assertions of parties in inter-state proceedings, the clean hands doctrine remains unsettled in international law and has rarely been applied.[76]

4. Necessity as a Circumstance Precluding Wrongfulness

Finally, even if it is established that Amestonia's seizure of the station and its equipment and/or its arrest of the three VoR employees constituted a wrongful act, Amestonia might still be able to claim "necessity" as a circumstance precluding wrongfulness. Amestonia would have to show, in accordance with Article 25 of the ILC Articles on State Responsibility, that its seizure and arrest were "the only way to safeguard an essential interest against a grave and imminent peril," that it "did not seriously impair an essential interest of Riesland," and that Amestonia "did not contribute to the situation of necessity."[77] Given the fact that the surveillance activity has been going on since 1992, it will be difficult for Amestonia to establish how its recent discovery of what had transpired constituted a "grave and imminent peril." Further, questions remain as to the extent to which Amestonia, by providing Frost with shelter and allowing for the continued leaks, possibly contributed to the situation of necessity.

---

[72] Note, that regardless of whether Articles 65-67 are reflective of customary international law, as both States are parties to the VCLT and as the BT was concluded after the two countries ratified the VCLT, those requirements are directly applicable.

[73] Note that a different strand of this argument could be to argue that Riesland abused its rights under the BT and is, thus, precluded from asserting any claims under it.

[74] BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS, 156 (1987).

[75] Factory at Chorzow, Jurisdiction, Judgment No. 8. P.C.I.J., Series A. No. 9, p. 31 (1927).

[76] ILC Articles on State Responsibility, *supra* note 22, at 72.

[77] *Id.*, at 80-84.

C. State Immunity Arguments

1. Jurisdictional Immunities of States and Their Property

Riesland National Television is a state-owned and operated corporation, which provides public broadcasting services across Riesland. In accordance with the BT, Riesland established a new division of the corporation, The Voice of Riesland (VoR), to operate in Amestonia. In accordance with Article 1(2) of the BT, the land on which VoR was established was acquired by Riesland and held under its name. Riesland also procured, at its own expense and in its own name, the necessary equipment for the station. As such, and regardless of the immunities provided for by the BT, Riesland may additionally claim that the VoR station and its equipment are Riesland's property and are immune from the civil jurisdiction of Amestonian courts.[78] Note that the pre-judgment measures of constraint, i.e. the seizure of property, were conducted under an emergency warrant pending a criminal investigation. As such, Riesland does not enjoy state immunity for these purposes as immunity over property does not extend to criminal jurisdiction.[79] The post-judgment measures of constraint. i.e. the forfeiture and potential auctioning of the property, are on the other hand civil acts, conducted outside of the prosecution of a defendant. It is in this context that state immunity might be applicable.

The ICJ in the *Jurisdictional Immunities* case established that the "commercial activity" exception to state immunity exists as a matter of customary international law, and that for measures of constraint to be taken "the property in question must be in use for an activity not pursuing government non-commercial purposes".[80] The *Compromis* is silent on the question of whether the VoR served any such commercial purposes. Amestonia will, thus, rely on the general commercial nature of TV broadcasting to enliven the exception.[81] Amestonia might further note that Carmen itself was used to advance Riesland's economic interests through espionage, further suggesting a commercial purpose to VoR's activities. Riesland will challenge this argument suggesting that the VoR station is distinct from other broadcasting facilities as it was established under a bilateral treaty for the sole purpose of

---

[78] BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 322 (6th ed.,1998).

[79] U.N. Convention on Jurisdictional Immunities of States and Their Property, G.A. Res.59/38 with commentaries, U.N. Doc.A/RES/59/38, Articles 5, 18-19 (2004). Commentary to Article 2 of the Convention clarifies that state immunity over property does not cover "criminal proceedings". The Convention has 28 signatories and 15 States have ratified or acceded. The Convention has not yet entered into force, and neither Amestonia nor Riesland are parties to it. Nonetheless, the Convention may be seen as "a catalyst for the development of the modern customary international law of State immunity". Both national and international courts have already looked to the Convection as persuasive evidence of custom. The ICJ itself relied on certain provisions of the Convention in its judgment in Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening), Judgment, ICJ Reports 2012. In a series of cases the ECtHR has applied the convention as customary international law (*see, e.g.*, Oleykinov v Russia, App. No. 36703/04, 14 March 2013, ¶ 66; Cudak v. Lithuania [GC], App. No. 15869/02, ECHR 2010, ¶¶ 67-74.

[80] Jurisdictional Immunities case, *Id.*, at ¶ 118.

[81] In *Los Angeles News v. Conus*, the U.S. District Court addressed the question of whether the Canadian Broadcasting Corporation (CBC) was entitled to immunity under the U.S. Foreign Sovereign Immunities Act. While CBC contended that its news broadcast, which relied on no advertisements and produced no profit, did not constitute commercial activity but was more akin to the production of academic or linguistic content. The Court rejected this claim noting that an activity needs not to be motivated by profit to be commercial and that the general nature of TV broadcasting involves commercial interests. *See Los Angeles v Conus*, 969 F Supp 579, 586 (CD Cal, 1997).

strengthening "political, cultural, and artistic" life. Its broadcasting of news and documentaries were, thus, all influenced politically and served solely governmental purposes with no commercial component.

Furthermore, in accordance with Article 15 of the United Nations Convention on Jurisdictional Immunities of States and their Property, Riesland may not invoke immunity in proceedings which relate to its participation in a company which has its seat or principle place of business in Amestonia. As the ILC clarifies: "when a State participates in a collective body, such as by acquiring or holding shares in a company... which is organized and operated in another State, it voluntarily enters into the legal system of that other State and into a relationship recognized as binding under that legal system. Consequently, the State is of its own accord bound and obliged to abide by the applicable rules and internal law of the State of incorporation, of registration, or of the principal place of business."[82] While the ILC provides citations to national and regional legislation that maintains this exception to immunity, Riesland may nonetheless challenge the customary nature of the exception enumerated in Article 15 to the Convention, given that both Amestonia and Riesland are not parties to it.

2. Immunity Ratione Materiae

Immunity *ratione materiae* applies to any government agent in respect of governmental acts.[83] This immunity accords with the "acts of state" doctrine which equates any act of an organ of the state with the state itself.[84] Regardless of their immunities under the BT, Riesland will contend that Mayer and the two VoR employees enjoyed immunity *ratione materiae* from the jurisdiction of Amestonia for all acts they performed on Riesland's behalf, including the Carmen Program. Amestonia will counter by looking to the vast practice of states exerting criminal jurisdiction over spies throughout history. Indeed in determining whether acts carried out by a State official are covered by immunity *ratione materiae* "the crucial consideration would be whether or not the territorial state had consented to the discharge in its territory of official functions".[85] Given that the Carmen program involved the covert hacking and surveillance of public officials without consent, allegedly by Mayer and the two VoR employees, the three are not entitled to state immunity for these actions.

D. Forfeiture/Expropriation and Unjust Enrichment

The prohibition of unjust enrichment is frequently cited as an example of a general principle of law under ICJ Statute Art. 38(1)(c).[86] The Iran-United States Claims Tribunal summarized the characteristics of unjust enrichment as follows: "There must have been an enrichment of one party to the detriment of the other, and both must arise as a consequence of the same act or event. There must be no justification for the enrichment, and no contractual or other remedy available to the injured party

---

[82] *ILC Draft Articles (with Commentaries) on the Jurisdictional Immunities of States, in* THE INTERNATIONAL LAW COMMISSION 1949-1998, VOLUME III: FINAL DRAFT ARTICLES OF THE MATERIAL 2078 (Sir Arthur Watts ed., 2000).

[83] *R v. Bow Street Metropolitan Stipendiary Magistrate, Ex parte Pinochet Ugarte (No 3),* 119 ILR 137, 205 (1999).

[84] *Attorney General of Israel v Eichmann,* 36 ILR 277, 308-309 (1962).

[85] Second Report on Immunity of State Officials from Foreign Criminal Jurisdiction, Special Rapporteur Roman Anatolevich Kolodkin, U.N. Doc. A/CN.4/631 ¶ 82 (10 June 2010).

[86] See, e.g., Libyan American Oil Company ('LIAMCO') Award of 12 April 1977 (LIAMCO v Government of the Arab Republic 62 ILR 141, 175–76 (12 April 1977).

whereby he might seek compensation from the party enriched."[87] Amestonia's intention to sell VoR's real estate and property, estimated to be worth €20 million, by public auction is within its *domaine réservé* and forms part of common police practice. Nonetheless, it may be challenged by Riesland as a form of unjust enrichment.

At the heart of the analysis is whether the enrichment was "justified." As some scholars have noted: "unjust enrichment remains an elusive legal phenomenon, combining ostensible mathematical simplicity with a high degree of legal ambiguity."[88] Amestonia may, thus, challenge the existence of a general principle or customary notion of "unjust enrichment," noting the different and varying types of factual situations to which the concept has been applied.[89] Alternatively, Amestonia may claim the exclusion of unjust enrichment in cases of wrongful conduct by the claimant. Applying the doctrine of *nemo auditur propriam turpitudinem suam allegans* ("no one will be heard relying on his own turpitude"), it has been firmly established in arbitration cases that "illegal or immoral conduct can defeat a claim of unjust enrichment which would otherwise lie."[90] Riesland's bad faith in spying might preclude it from raising an unjust enrichment claim. In a similar manner, in the context of expropriation proceedings it has been widely accepted that no compensation will be granted where the confiscation was taken as a penalty for a domestic crime.[91]

---

[87] The Iran-United States Claims Tribunal, Sea-Land Service Inc. v. Iran, 6 Iran-US Claims Tribunal Reports, 149, 169 (Grotius Cambridge, 1986).

[88] Christina Binder & Christoph Schreuer, *Unjust Enrichment*, Max Planck Encyclopedia of Public International Law, *available at* https://goo.gl/eej5xx.

[89] *Id.*

[90] Gerhard Dannemann, *Illegality as Defence against Unjust Enrichment Claims*, *in* UNJUST ENRICHMENT: KEY ISSUES IN COMPARATIVE PERSPECTIVE 310 (Reinhard Zimmermann and David Johnston eds., 2002).

[91] JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 624 (Oxford University Press, 8th ed, 2012).

III. THE LEGALITY OF PREVENTIVE DETENTION AND THE DISCLOSURE OF SECRET EVIDENCE

QP3 asks the teams to first present arguments on the legality of preventive detention in the context of the travails of the former politician Joseph Kafker, who was apprehended on 7 March 2015 in accordance with Riesland's detention powers under its "Terrorism Act." Preventive detention is the detention of persons without charge, and it has been increasingly used by many nations as a tool to fight terrorism in the aftermath of the attacks in New York City of 11 September 2001.[92] Teams will then have to analyze whether Riesland can be mandated by the court to release Kafker and hand over the secret evidence from the closed proceedings against him.

Applicant's Prayer for Relief	Respondent's Prayer for Relief
Joseph Kafker's detention is substantively arbitrary and it violates guaranteed procedural safeguards enshrined within international human rights law. Further, the public emergency exception does not apply here and Riesland may not derogate from its obligations under the ICCPR. Finally, Amestonia is entitled to view the evidence currently held against Joseph Kafker.	Joseph Kafker is legally and properly detained and Riesland has afforded him all due process rights under international human rights law while in an on-going state of emergency. Finally, Riesland is not obligated to present Amestonia or the Court with the secret evidence it holds against Kafker.

A. The Legality of Preventive Detention under the ICCPR

1. The Right to Personal Liberty and the Prohibition of Arbitrary Detention

Article 9(1) of the ICCPR states that: "Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law."[93] The third sentence requires that the detention be ordered under grounds stated in domestic law and enacted via procedure stated in domestic law (firmly grounded in the principle of legality or *nullem crimen sine lege*).[94] The Terrorism Act domestically legalizes Kafker's detention, and his detention has accorded with the procedures laid forth in the Act, satisfying the principle of legality. Here, however, since Article 9(1) applies fully to the detention, pleaders for both sides will have to discuss whether the detention of Joseph Kafker is substantively "arbitrary."

---

[92] A non-exhaustive list of nations with preventive detention systems includes the United States, United Kingdom, Brazil, Colombia, France, Israel, Germany, Italy, Norway, Greece, Ireland, Spain, and Turkey. For further reading *see* CLAIRE MACKEN, COUNTER-TERRORISM AND THE DETENTION OF SUSPECTED TERRORISTS: PREVENTIVE DETENTION AND INTERNATIONAL HUMAN RIGHTS LAW 2 (Kindle Edition, 2011).

[93] International Covenant on Civil and Political Rights, 999 U.N.T.S. 171, Article 9(1) (1966).

[94] Yoram Dinstein, *Right to Life, Physical Integrity and Liberty*, *in* THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 130 (Louis Henkin ed., 1983).

Neither a specific definition of "arbitrary," nor specific examples of what "arbitrary" is or what types of detention it applies to, are provided in the text of the ICCPR.[95] The task lay with the HRC, as the primary interpretive body of the ICCPR,[96] to flesh out its meaning. In General Comment 35 on ICCPR Article 9, the HRC noted that the notion of arbitrariness must be interpreted to include "elements of inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity, and proportionality."[97] Thus, students will have to examine whether or not the preventative detention of Kafker is reasonable, necessary, and proportionate to achieve the aim of protecting Riesland's national security.

To address this issue teams may look to whether any reasonable grounds existed to believe that Kafker was involved in terrorist activity, and whether there was any likelihood of the future commission of a crime by Kafker in light of relevant information and past behavior.[98] Amestonia will note there is an absence of concrete evidence linking Kafker to the Hive's attacks, aside from a number of visits to the longlivethehive website and him using the "like" function on posts which called for violent disruptions as a mean of public awareness. Riesland, on the other hand, will cite the memorandum of Attorney General Deloponte which establishes the existence of "closed materials" that cannot be disclosed linking Kafker to the honey contamination plot and to the hive's senior echelons.[99]

In *D. and E. v Australia*, the HRC noted that for a detention to be proportionate a State must demonstrate that other, less intrusive, measures could not have achieved the same end.[100] Amestonia may try to argue against Kafker's detention in a maximum-security facility by suggesting that less-forceful non-custodial alternatives (house arrests, electronic monitoring bracelets, etc.) were available to Riesland.

---

[95] Contrast this with the European Convention on Human Rights and Fundamental Freedoms, that lists specific instances of when a person may be detained under its analogous right to liberty, provided in Article 5(1) subparagraphs (a)-(f). Particular relevance lies with subparagraph (c) which reads: "the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so."

[96] *See* Diallo, *supra* note 58, at ¶ 66 ("Since it was created, the Human Rights Committee has built up a considerable body of interpretative case law, in particular through its findings in response to the individual communications which may be submitted to it in respect of States parties to the first Optional Protocol, and in the form of its "General Comments". Although the Court is in no way obliged, in the exercise of its judicial functions, to model its own interpretation of the Covenant on that of the Committee, it believes that it should ascribe great weight to the interpretation adopted by this independent body that was established specifically to supervise the application of that treaty. The point here is to achieve the necessary clarity and the essential consistency of international law, as well as legal security, to which both the individuals with guaranteed rights and the States obliged to comply with treaty obligations are entitled").

[97] Human Rights Committee, General Comment 8, U.N. Doc HRI/ GEN/1/Rev.6, ¶¶ 1-5 at 130 (2003); *See also* Hugo van Alphen v The Netherlands, HRC Comm No 305/1988, 23 July 1990, CCPR/C/39/D/305/1988, ¶ 5.8 (1990).

[98] *David Alberto Cámpora Schweizer v. Uruguay*, Comm. No. 66/1980, ¶¶ 3.3, 3.5 (1990).

[99] Note a potential conflict here between QP1 and QP3; For Riesland to rely on the memorandum here would assume it accepted it as reliable and admissible.

[100] *D and E and their two children v. Australia*, Comm. No. 1050/2002, U.N. Doc. CCPR/C/87/1050/2002, ¶ 7.2 (2006).

Teams will further have to analyze the other procedural safeguards laid down in ICCPR Articles 9(2)-9(4), namely: (1) the right to be informed, during an arrest, of the reasons of the arrest; (2) the right to a prompt trial; and (3) the right to challenge detention through a judicial proceeding.

a. The Right to be Informed - Article 9(2)

Article 9(2) requires that detainees be informed of the reasons for their arrest. In *Adolfo Drescher Caldas v. Uruguay*, the HRC held that the ICCPR "requires that anyone who is arrested shall be informed sufficiently of the reasons for his arrest to enable him to take immediate steps to secure his release if he believes that the reasons given are invalid or unfounded."[101] Uruguay had informed Drescher Caldas that he was held under security measures and gave no further information on the substance of the allegations. The HRC found this violated Article 9(2). However, in the *Diallo* case the ICJ noted that a decree notifying Diallo that his arrest was for the purpose of "an expulsion procedure" would have been sufficient to meet the requirements of Article 9(2) as it would have allowed him "to take appropriate measures to challenge the lawfulness of the decree."[102]

At the time of his arrest, Kafker was merely informed that the arrest was "in accordance with the Terrorism Act". Indeed §3(a) of the Act establishes that the Rieslandic Government may detain "any foreign national suspected of being involved in instigating, planning, financing, carrying out, or aiding a terrorist act." When brought before the Tribunal, Kafker's detention was further extended for reasons of "national security," as allowed under §3(d) of the Act. Riesland may try to argue that both these statements provide for sufficient notification, as they resemble the ICJ's preposition in Diallo (by providing Kafker with the overarching reasons for the detention and allowing Kafker the possibility to challenge the detention's lawfulness). Amestonia will counter that Kafker's notification must involve more than just the mere legal basis for the detention. §3(a) of the Terrorism Act is too broad to constitute sufficient notification, and simply citing to "national security" reasons has already been deemed by the HRC to be insufficient to meet the requirements of Article 9(2).[103]

b. The Right to a Prompt Trial - Article 9(3)

Article 9(3) requires that "anyone arrested or detained on a criminal charge shall be brought promptly before a judge or other officer authorized by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release." Teams must first address whether the Article is applicable to Kafker. The HRC confirmed in *Vladimir Kulomin v. Hungary* that Article 9(3) applies to detainees held only under criminal jurisdiction.[104] In General Comment 8 to Article 9, the Committee reiterated that all of Article 9(3) applies only in the case of a criminal matter.[105] As Riesland has not

---

[101] *Adolfo Drescher Caldas v. Uruguay*, Communication no. 43/1979, U.N. Doc. Supp. No. 40 (A/38/40), ¶ 13.2 (11 January 1979).

[102] *See* Diallo, note 58, at ¶ 84.

[103] *Willy Wenga Ilombe and Nsii Luanda Shandwe v Democratic Republic of the Congo*, Comm. No. 1177/2003, U.N. Doc CCPR/C/86/D/1177/2003, ¶ 6.2 (2006).

[104] *Vladimir Kulomin v Hungary*, Comm. No. 521/ 1992, U.N. Doc. CCPR/C/50/D/521/1992, ¶ 1 (22 March 1996).

[105] General Comment 8, *supra* note 97, ¶ 3. Note that the HRC did note that pre-trial detention should be "an exception and as short as possible".

charged Kafker with a crime yet, but is rather holding him under preventive detention, this Article does not seem to apply. Consequently, Riesland can argue that preventive detention is not subject to this positive obligation to provide a speedy proceeding unless criminal charges are filed. Amestonia may refer to Wennerg's separate opinion in *Kelly v. Jamaica*, in which he argued that Article 9(3) applied fully to preventive detention.[106] The ICJ has taken a similar approach in the *Diallo* case.[107] Indeed a restrictive interpretation of Article 9(3) would likely only defeat its purpose of procedural fairness and further incentivize States to evade responsibility by not charging detainees.[108] Amestonia may also note that the analogous Article 5(3) of the European Convention on Human Rights makes no reference to criminal charges and applies a general requirement of promptness of trial to all detainees equally.[109]

As of 15 January 2016, Kafker has been detained for 315 days. By 1 April 2016 he would have been detained for over a year (390 days) without any charges being brought up against him, let alone the commencement of trial proceedings. Amestonia may argue that Kafker's right to a speedy investigation and trial has been violated. The ECtHR in *Beretesegi et al v. France* ruled that the extended pre-trial detention of alleged terrorists (in that case detentions of Basque separatists members of the ETA for periods of between four and five years) was unreasonable as there were no particular compelling reasons to justify the delay. Therefore, states are required to show that they are using the extended time to gather evidence and investigate, directly linking "the length of the pre-trial detention at issue... to the complexity of the cases."[110]

Amestonia can argue here that Riesland similarly has provided no justifications for its prolonged detention of Kafker, while routinely extending his detention by solely referencing vague "national security" interests. Riesland has not provided any evidence of its continuing investigation and, at any rate, refuses to release such evidence to Kafker, Amestonia, or the Court. Riesland will respond that the length of the pre-trial detention must be weighed against the need for Riesland to adequately prepare for the case given the seriousness of terrorism charges. Riesland would cite to §3(d) of the Terrorism Act, which provides specific factors for the National Security Tribunal to consider in granting a request for an extension of the detention, which might further shed light on the justifications for the extensions. Riesland may also note that the act itself clarifies that detention cannot be extended over 540 days, setting an ultimate limit for its investigation.

---

[106] *Paul Kelly v. Jamaica*, Comm. No. 253/1987, U.N. Doc. CCPR/C/41/D/253/1987 (10 April 1991). Note, however, that the merits in that case were eventually decided under Article 14(3) of the ICCPR and did not concern itself over expanding 9(3)'s application to preventive detention.

[107] *See* Diallo, *supra* note 58, at ¶¶ 82 (noting to the fact that Mr. Diallo "was held for a long period of time" and suggesting that such time, without an attempt by the authorities to establish why the detention was necessary, might constitute an arbitrary detention within the meaning of Article 9 of the ICCPR).

[108] NIGEL RODLEY, THE TREATMENT OF PRISONERS UNDER INTERNATIONAL LAW 335-336 (2000).

[109] Article 5(3) reads: "Everyone arrested or detained in accordance with the provisions of paragraph 1(c) of this Article shall be brought promptly before a judge or other officer authorized by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial."

[110] European Court of Human Rights, *Excessive Length of Pre-Trial Detention of ETA terrorists Breached the Convention, Press Release*, ECHR 032 (26 January 2012), *available at* https://goo.gl/Icmtfk.

c. The Right to Judicial Review - Article 9(4)

Article 9(4) establishes that anyone deprived of his liberty is entitled to take proceedings before a court in order for that court to decide the lawfulness of his detention and order his release if the detention is unlawful. Amestonia may, thus, challenge the extent to which the judicial review offered by the National Security Tribunal meets the requirements of Article 9(4).

In *Kirpo v. Tajikistan*, the HRC said that under Article 9(4) the judicial authority had to be "independent, objective and impartial in relation to the issues dealt with."[111] Teams may argue the extent to which the National Security Tribunal meets requirements of independence and impartiality. Riesland will note that the Tribunal is a five-judge judicial authority with the competence to "decide the lawfulness of the detention and to release the detainee if found that the detention is unlawful," thus, meeting the technical requirements of Article 9(4).[112]

Amestonia may rely on the fact that the five judges who sit on the tribunal are responsible to both review the surveillance programs and the detention procedures. In other words, the same judges who authorized Kafker's surveillance under the SSBA, and who never once challenged the Carmen program which was used to obtain the secret evidence against Kafker, are now routinely extending his detention under the Terrorism Act, casting doubt on their impartiality. Furthermore, Amestonia may note that in accordance with §3(c) of the Act, the proceedings before the Tribunal are secret and its records not open to public scrutiny. Finally, Amestonia may recall the fact that when Kafker tried to challenge his detention and the proceedings before the Rieslandic Supreme Court, he was denied.

Proceedings under Article 9(4) must also entertain the requirement of procedural fairness. As the ECtHR explained in *A v. U.K.* while there is no uniform standard, proceedings must ensure "equality of arms between the parties."[113] In the present case, Kafker may only select his counsel from a list of pre-authorized "special advocates". He is also not privy to the "closed materials" levied against him as this evidence is only available for his counsel to examine but not share with Kafker. Consequently, Kafker is prevented the opportunity to examine witnesses within his presence. Teams will argue on the fairness of these measures, and whether the adversarial process is indeed protected.

In *Chahal v. U.K.,* the ECtHR recognized that the use of confidential material "may be unavoidable where national security is at stake." The Court, nonetheless, ruled that States have a requirement to seek techniques, that "both accommodate legitimate security concerns about the nature and sources of intelligence information [while] accord[ing] the individual a substantial measure of procedural justice."[114] Teams may turn to similar terrorism laws, which rely on "closed materials" and on restrictions on "choice of attorney", to determine whether alternative techniques were indeed available to Riesland.

---

[111] *Kirpo v. Tajikistan*, Comm. No. 1401/2005, U.N. Doc. CCPR/C/97/D/1401/2005, ¶ 6.5 (3 December 2009).

[112] *A v. The United Kingdom*, App. No. 3455/05, Grand Chamber Judgment, ¶ 202 (19 February 2009)

[113] *Id.*, at ¶¶ 203-204.

[114] Chahal v. The United Kingdom. App. No. 22414/93, Judgment, ¶ 131 (15 November 1996).

B. The Legality of Preventive Detention in Times of Public Emergency

Under Article 4(1) of the ICCPR, a state may derogate from certain rights enumerated under the ICCPR during public emergencies.[115] Accordingly, Riesland may derogate from its obligations under Article 9, as above listed, if it can validly show that it was experiencing a "public emergency, which threatened the life of the nation."

1. The Existence of a Public Emergency

The term "public emergency" is not specifically defined in either Article 4 or its analogue within the ECHR, Article 15. Definitions from the HRC and the ECtHR are therefore of use in determining the meaning of the term. In the *Greek* case, the ECtHR defined a public emergency as one that was actually occurring or imminent, whose effects involved the entire nation and threatened the continued organized life of the community.[116] Further, the ECtHR stated that the crisis or danger must be such that normal measures or restrictions for the maintenance of public safety, health and order, are plainly inadequate.[117] The HRC also stressed that public emergencies must be "exceptional,"[118] namely, actual imminent threats affecting the whole population and endangering the nation's existence.[119] In the *Lawless* case, the ECtHR held that a non-state actor's continued violent activities constituted a public emergency.[120] Further, in the *Ireland* case, the ECtHR ruled that national authorities are best suited to decide on whether an emergency exists and what derogations are necessary.[121]

Riesland can argue that it was in the midst of a public emergency after two of its citizens died (2 February 2014), and its ministers and businessmen were threatened with poison (7 March 2014). It further helped thwart a terrorist attack against its citizenry by The Hive, who had planned to contaminate Amestonian honey intended for Rieslandic consumption (16-21 October 2014). In more than 50 additional incidents, Riesland provided Amestonian security authorities with information concerning terrorist activity that threatened both countries.

Amestonia can argue that none of this constitutes a public emergency, as the ECtHR ruled in the *Greek Case* that bombings and sabotage alone are not a threat to the nation's life.[122] Further, Amestonia can question the imminence of the attacks and whether they were of a character to harm the life of the nation. For example, the bombings in question occurred outside Riesland's territory and the sabotage

---

[115] ICCPR, *supra* note 93, Article 4(1).

[116] *Denmark, Norway, Sweden and the Netherlands v. Greece*, Case Nos. 3321/67, 3322/67, 3323/67 and 3344/67, EComHR, Dec. & Rep. 5, ¶¶152-3 (1968) (The *Greek* Case).

[117] *Id.*

[118] Human Rights Committee, General Comment 29, U.N.Doc.CCPR/C/21/Rev.1/Add.11, ¶ 2 (2001).

[119] The *Greek* Case, *supra* note 116, at ¶¶ 152-3 (1968); *Lawless v. Ireland*, Case No. 332/57, 3 ECtHR, p.29 (1961).

[120] The *Greek* Case, *Id.* at ¶¶ 101-102.

[121] *Ireland v. U.K.*, Case No. 5310/71, 25 ECtHR, ¶¶ 207 (1978).

[122] The *Greek* Case, *supra* note 116, at ¶¶142-4.

was eventually thwarted (note further that the arrested individuals insisted that the chemically altered neonicotinoids posed no threat despite the subsequent police investigation concluding otherwise). Amestonia may further argue that even if the initial terrorism alert was justified, the continued alerts and derogations are invalid, as the *Compromis* includes no evidence of any further activity by The Hive after October 2014. It may therefore be questionable whether Riesland can claim an imminent threat in order to justify Kafker's proceedings, which began 7 March 2015, approximately 5 months after the thwarted attack of 21 October 2014. Riesland will respond that it is precisely because of the measures it employed that no threats had actually materialized.

2. Valid Notice of Derogations

Even if a state is permitted to derogate from the ICCPR, it must immediately notify other parties to the ICCPR of its derogations and provide justifications under Article 4.[123] The *Compromis* makes no mention of Riesland having complied with these notice requirements. Further, Riesland simply issued terrorism alerts rather than explicit declarations of a "state of emergency" accompanied by formal notification. However, Riesland can argue that, in light of rulings by multiple international tribunals, a formal notification may be waived, as broader public emergency declarations are sufficient.[124] The act of proclamation involves a state's publicized decision to ensure thorough political deliberations regarding the extent of rights derogated.[125] Here, Riesland declared a Terrorism Alert that openly publicized an imminent threat to its nation, as per the statutory language of the Terrorism Act. Furthermore, Riesland has notified the Secretary General of the United Nations of each of its issued alerts, as is required under the ICCPR.

3. Derogations Strictly Limited to the Exigencies of the Situation

Even if a state has given proper notice, its derogations must be proportional to the factual circumstances. The severity, duration, and geographic scope of derogations are permissible only to the extent that they are strictly required by the exigencies of the situation. This requires that derogations be necessary and proportionate to the threat.[126] Further, derogations must be temporary and able to accomplish the legislative objectives of the emergency declaration.[127] Amestonia can argue that the exigencies of this situation did not require the deprivation of rights and liberty inherent to the detention structure established by the Terrorism Act. It can argue that any and all terrorist attacks ended on 21 October 2014 with the arrest of the planners of the honey contamination scheme. Amestonia can argue that there was no justifiable, exigent circumstance, mandating the detention of a retired Amestonian

---

[123] ICCPR, *supra* note 93, at Article 4(3).

[124] *Cyprus v. Turkey* App. Nos. 9780/74, 6950/75, 4 EComHR, para.527 (1976); *Silva. v. Uruguay*, Comm. No. R.8/34, U.N. GAOR, Supp. No. 40, U.N. Doc. A/36/40 130, ¶ 8.3 (1981); *Ramirez v. Uruguay*, Comm. No. 4/1977, U.N. Doc. CCPR/C/10/D/4/1977, ¶ 17 (1980).

[125] *Cyprus v. Turkey*, *Id.*, Dissenting Opinion of Judge Sperduti, ¶ 4.

[126] U.N. Economic & Social Council, Siracusa Principles on the Limitation and Derogation of Provisions in the ICCPR, Annex, U.N. Doc.E/CN.4/1984/4, ¶ 51 (1984); General Comment 29, *supra* note 118, ¶ 6; JAIME ORAÁ, HUMAN RIGHTS IN STATES OF EMERGENCY IN INTERNATIONAL LAW 152-168 (1992).

[127] Siracusa Principles, *ibid.*, ¶¶ 48-51; ORAÁ, *ibid.*, p.154; *A (FC) v. Secretary of State*, UKHL 56 EWCA (Civ) 1502, ¶ 30 (2004).

politician six months after the thwarted attack and that there was less justification for the subsequent deprivation of his procedural guarantees to be notified of the charges against him, review evidence, choose counsel, and challenge the lawfulness of his detention.

Although states must show this proportionality by rationally linking the emergency and derogative measures and proving that no less restrictive measure exists, Article 4(1) leaves substantial room for state discretion.[128] Riesland may argue that its actions in this case fall within the exercise of its margin of appreciation. Furthermore, Riesland can once more point to the recent lack of attacks as evidence of the success of its national security system.

4. Non-Derogable Rights

Even if a state of emergency is sufficiently established, Riesland may still not derogate from certain rights as enshrined under the ICCPR. While Articles 9 is derogable, the HRC added two important clarifications in General Comment 29.[129]

a. "Fundamental Principles of Fair Trial"

The HRC clarified in General Comment 29 that: "States parties may in no circumstances invoke Article 4 of the Covenant as [a] justification for acting in violation of humanitarian law or peremptory norms of international law" either "through arbitrary deprivations of liberty [deviations] from fundamental principles of [a] fair trial, including the presumption of innocence." In its Concluding Observations on Israel, relating to the latter's policies of administrative detention, the HRC noted that "a State may not depart from the requirement of effective judicial review of detention".

While the Covenant itself does not consider the rights enumerated in Article 9 to be non-derogable, the HRC seems to take a different approach, suggesting that certain elements within the right might actually be non-derogable. To the extent that Amestonia is able to claim that the right to choose counsel, the right to be informed, the right to a prompt trial, the right for an independent and impartial judicial review, or the right to examine evidence, are rights of such a "fundamental" character, then Riesland may not be able to derogate from those rights and therefore may not rely on the "public emergency" to justify its actions.

b. "Dimensions of the Right of Non-Discrimination"

The HRC further clarified that one of the "conditions for the justifiability of any derogation from the Covenant is that the measures taken do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin." The HRC determined that there are "elements or dimensions of the right to non-discrimination that cannot be derogated from in any circumstances." Specifically, the HRC noted that this would apply if "distinctions between persons [were] made when resorting to measures that derogate from the Covenant." Section 3(a) of the Terrorism Act states that the Government may apply its "detention powers" only against "foreign nationals." Thus, the act may be said to make "distinctions between persons." Riesland may counter that such a distinction on the basis of nationality is common in the practice of counter-terrorism laws among

---

[128] *Ireland v U.K. supra* note 121, ¶ 207; *Lawless, supra* note 119, at pp. 310-312.

[129] General Comment 29, *supra* note 118, ¶¶ 8, 11.

states, and that the distinction was also necessary and relevant given that the risk of terrorist activity Rielsand was facing emanated predominately from beyond its borders.

C. Remedies: The Release of Kafker, Disclosure of Evidence, and Compensation

1. Kafker's Immediate Release

The right to release from unlawful detention is inherent to Article 9 of the ICCPR.[130] Furthermore, restitution is the primary form of reparation and involves the establishment of the situation that existed before the wrongful act was committed.[131] The restoration of Kafker would, thus, restore the *status quo ante*. Riesland may claim that an order demanding the release of Kafker would constitute an impermissible intrusion into Riesland's domestic affairs. As in *Avena*,[132] Riesland should only be obliged to "review and reconsider" Kafker's detention by means of its own choosing, rather than be ordered to release him. For example, Riesland may decide to charge Kafker and launch criminal proceedings against him, an act that will also correct the wrong produced by its pre-trial detention.

2. Disclosure of Evidence

Amestonia will request that the Court order Riesland to produce the intelligence that formed the basis of Kafker's detention, notwithstanding its highly classified status. Amestonia will further argue that Riesland should not be allowed to rely on the intelligence to support its claims in this case if it fails to produce such evidence. Article 49 of the ICJ Statute states that the Court may, even in a pre-hearing phase, "call upon the agents to produce any document or to supply any explanations" and that "formal note shall be taken of any refusal." Although the Court may call upon a party to produce evidence, Article 49 does not empower the Court to compel the production of evidence. Thus, even if the ICJ calls upon Riesland to produce the intelligence, Riesland may refuse.[133]

Amestonia will argue that the overriding interest of justice requires the Court to assert that Riesland has a duty to produce the intelligence data, and to request that Riesland produce the evidence in satisfaction of that duty.[134] The intelligence is integral to the case and the Court has to avail itself of all

---

[130] Human Rights Committee, General Comment 35, U.N. Doc. CCPR/C/GC/35 (16 December 2014).

[131] ILC Articles on State Responsibility, *supra* note 22, at 35.

[132] Avena and Other Mexican Nationals (Mexico v. US), Judgment, ICJ Rep. 1, ¶ 125 (2004).

[133] Application of the Convention on the Prevention and Punishment of the Crime of Genocide Bosnia and Herzegovina v. Serbia and Montenegro, Merits (Diss. op. Mahiou), ICI 2007 (stating that there is no obligation concerning cooperation in evidentiary maters in the Statute or Rules of the Court and that any such cooperation is an act of good faith by the relevant party). There has been a historical reluctance to empower the Court with fact-finding authority that would be in tension with state sovereignty. When revising the Rules of the PCIJ of 1936, the Second Committee questioned whether it was "possible to say anything [in the Statute or Rules of Court] about the duty of a party to produce all relevant information in its possession." The Second Committee considered it best to refrain from affirming the existence of a duty to produce all relevant information in the possession of the parties because "governments must claim to exercise occasionally the right to refuse to produce a document on the ground of public interest, and of that interest it claims to be the sole judge," concluding that "the matter will have to be regulated in the future by a convention."

[134] Barcelona Traction. Light and Power Company, Limited (Belgium v. Spain), Preliminary Objections (Sep. op. Bustamante), 1964 ICJ 78, 80 (1964) ("I naturally accept that in each case the onus of proof is placed on one of the parties,

possible evidence and resources available to it under its Statute and Rules. Riesland may argue that the production of highly classified information will infringe on its sovereignty and harm its national interests. It may further note that ordering the release of the information will be excessively burdensome making it an inappropriate measure of reparation for procedural breaches of the ICCPR.[135]

3. Compensation

Article 9(5) of the ICCPR requires that detainees be provided with compensation if unlawfully detained. In *A. v. Australia*, the HRC confirmed that compensation must also be paid even if a detention was legal under domestic law but contrary to the ICCPR.[136] The ICJ, in the *Diallo* case, awarded material and non-material damages as a result of arbitrary detention.[137] Under rules of diplomatic protection Amestonia is entitled to the awards on behalf of Kafker.

---

but it is also true that the overriding interests of justice give the Court the faculty of taking such steps as are possible to induce the parties to clarify what is not sufficiently clear.").

[135] Pulp Mills on the River of Uruguay (Argentina v. Uruguay), Judgment, ICJ Rep 14, ¶ 274 (2010).

[136] *A v. Australia*, Comm. No. 560/1993, U.N. Doc. CCPR/C/59/D/560/1993, ¶ 9.5 (30 April 1997).

[137] *See* Diallo, *supra* note 58, at ¶ 21.

IV. THE ATTRIBUTION AND LEGALITY OF A LOW-INTENSITY CYBER ATTACK

QP4 calls on teams to address two issues surrounding current legal scholastic debates around cyber security: (1) under what circumstances can a cyber attack be attributable to a state; and (2) what potential breaches of international law might ensue from a one-off, low-intensity cyber strike. NATO's International Group of Experts who produced the Tallinn Manual 1.0 is examining these two issues, and is expected to release a second version of the Tallinn Manual in the latter part of 2016. Legal research of these issues will depend on recent state practice, as well as various instances of soft law, to establish the existence of emerging norms concerning attribution and legality in cyber sphere.

To fully examine these issues substantively, students may turn to an array of potential legal arguments, many of which have merit. ***Judges are encouraged both to provide students with the space to flexibly experiment with these alternative arguments, as well as to guide them towards those arguments that judges find most compelling or intriguing.***

Applicant's Submission	Respondent's Submission
The cyber attack against an Amestonian newspaper and law firm was both attributable to Riesland and constituted a wrongful act. Even if the attack is not directly attributable to Riesland, Riesland is liable for failing to uphold standards of due diligence in preventing such an attack.	Riesland is not responsible for the cyber attack, as the attack was not attributable to it and, in any event, did not violate any international obligation owed to Amestonia.

A. Riesland's Responsibility for the Attack

1. Direct Attribution of the Attack to Riesland

Article 4 to the ILC Articles on the Responsibility of States for Wrongful Acts, which reflects customary international law,[138] attributes to the State the conduct of its organs, regardless of their function or position within the organization of the State.[139] While the SSBA does not explicitly define the Bureau as an organ of the State, it is clear that it exercises executive functions, controlled through both legislative and judicial oversight mechanisms, represents Riesland in various bilateral meetings (including in the context of intelligence sharing), and coordinates with other Rieslandic State ministries

[138] Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion, I.C.J. Reports 1999, ¶ 62 (referring to the draft articles on State responsibility, article 6, now embodied in article 4) ("according to a well-established rule of international law, the conduct of any organ of a State must be regarded as an act of that State. This rule... is of a customary character").

[139] ILC Articles on State Responsibility, *supra* note 22, at 40-42.

and positions (including the Minster of Foreign Affairs and the Attorney General).[140] A problem exists, however, in establishing the link between the Bureau and the cyber attack. Amestonia will need to argue for a lowered evidentiary standard both in the context of cyber operations, and in light of Riesland's full control over the evidence. Amestonia will then have to show that the circumstantial evidence provided in the case is sufficient to lead to a conclusion of attribution.

a. The Case for Lowered Evidentiary Requirements in Cyber Law

The general maxim of *Onus Probandi Incumbit Actori* (the burden of proof is on the claimant) is not an absolute one. The ICJ itself identified in *Diallo* that "the determination of the burden of proof is in reality dependent on the subject-matter and the nature of each dispute brought before the Court" varying with the facts of the case."[141] Separate from the question of which side bears the burden, the Court must also determine what should be the actual standard of proof. The Iran-United States Claims Tribunal has affirmed, and the ILC in its Articles on Responsibility of States has adopted, that: "in order to attribute an act to the State, it is necessary to identify with *reasonable certainty* the actors and their association (emphasis added)."[142]. In the *Corfu Channel* case, however, the ICJ took a different position, noting that: "the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility," adding that such states "should be allowed more liberal recourse to inferences of facts and circumstantial evidence" as such "indirect evidence is admitted in all systems of law, and its use is recognized by international decisions."[143]

Attribution in the cyber-sphere is riddled with difficulties and it is practically impossible to attribute cyber activities with unqualified certainty to a particular State actor. Hackers can mask or spoof the originator, and make it difficult for cyber-security experts to trace their activities.[144] "As an example,

---

[140] As the Tallinn Manual itself clarifies: "any cyber activity undertaken by the intelligence, military, internal security, customs, or other State agencies will engage State responsibility" (*see* MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 31 (2013).

[141] *See Diallo*, *supra* note 58, at ¶¶ 54-55.

[142] Kenneth P. Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R., vol. 17, pp. 101-102 (1987); ILC Articles on State Responsibility, *supra* note 22, at 39.

[143] *See* Corfu Channel, *supra* note 8, at p. 18. Note, however, that Riesland may rely on the more recent Crime of Genocide case wherein the Court in its majority opinion rejected the position laid out by Judge Lauterpacht in his separate opinion, and instead relied far less on circumstantial evidence. Indeed while the Court found circumstantial evidence from the UK reliable enough to hold Albania legally responsible, it did not find Bosnia's circumstantial evidence reliable enough to decide that Serbia intended to commit genocide. For an analysis of these two cases and a possible reconciliation between them, *see* Michael P. Scharf & Margaux Day, *The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences*, 13(1) CHI. J. INT'L L. 123, 142-143, 149-151 (2012).

[144] *See, e.g.*, Nicholas Tsagourias, *Cyber Attacks, Self-Defense, and the Problem of attribution*, 17(2) J. CONFLICT & SEC. L. 1, 6-8 (2012) ("Three particular characteristics of cyberspace make attribution extremely difficult. The first is 'anonymity' in that cyber attackers can hide their identity; the second is the possibility of launching multi-stage cyber attacks, in that a number of computers operated by different people and placed in different jurisdictions are infiltrated before an attack is launched; and the third is the speed with which a cyber attack can materialize. What is critical, then, is not only to trace back the attack to its source, for example to a computer, but to identify the person who operated the computer, and more importantly to identify the real 'mastermind' behind the attack; and it is especially critical that all of the above are done in a timely manner and accurately... This however gives rise to questions about the availability and the probity of evidence upon which assessments are made.").

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 the second State is responsible for them."[145] This was indeed the case in the context of Estonia (2007) and Georgia (2008).[146] Given the current architecture of the Internet with its countless loopholes that it provides, some scholars favor a lowering of evidentiary standards in cyberspace, stating that adequate attribution is a "luxury unavailable in the cyber attack era."[147] Others have rejected these proposals, noting that they can "hardly be considered legally tenable," referencing the widespread agreement that international law as it currently stands should apply just the same in cyber sphere, including with reference to standards on attribution.[148]

b. Riesland's Responsibility for the Attack

Amestonia will argue that given the unique features of cyber space, and owing to the "exclusive control" that Riesland holds over evidence relating to the cyber attack, the burden of proof should shift and lowered evidentiary standards should apply. Amestonia will then rely on the report produced by security experts from the Amestonian Institute of Technology, a world renowned research intensive academic institution, which (a) traced the malware used in the hacking to IP addresses within Riesland's territory; (b) associated those IP addresses with Rieslandic computer infrastructures; and (c) found significant segments of code in the malware to be exact replicas of those used in "Blaster", a previous malware software used by the Bureau. Furthermore, Amestonia will note that Riesland had the most to gain from the disruption of *The Ames Post* and Chester & Walsingham's computer systems and subsequent corruption of their data. Amestonia can also point to the facts that only 8 days prior to the hack, Riesland's Attorney General publicly stated that Riesland would do "whatever is in its power to disrupt" any further leaks, and that the hack came only five days after yet another leak by *The Ames Post*. Amestonia will argue it should be "allowed more liberal recourse to inferences" given that these are "a series of facts linked together and leading logically to a single conclusion."[149]

Additionally, Amestonia may refer to the practice of certain States, such as the United States., in the attribution of similar cyber attacks. In the context of the North Korean hack on Sony (2014), the Chinese hack of the Office of Personnel Management (2014-2015), and the Russian hack of the Pentagon (2015), a pattern has emerged. The U.S. openly blamed those countries for the hacks, justifying its conclusions on technical analysis performed by the FBI, which either traced IP addresses

---

[145] Michael N. Schmitt, *Cyber Activities and the Law of Countermeasures*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 659, 685 (Katharina Ziolkowski ed., 2013).

[146] Tallinn Manual, *supra* note 140, at 35.

[147] Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 232 (2002); Sean M. Condron, *Getting it Right: Protecting American Critical Infrastructures in Cyberspace*, 20(2) HARV. J. L. & TECH. 403, 415 (2007).

[148] Robin Geiß & Henning Lahmann, *Freedom and Security in CyberSpace: Shifting the Focus Away From Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 621, 627-628 (Katharina Ziolkowski ed., 2013).

[149] *See* Corfu Channel, *supra* note 8, at p. 18.

back to those countries, found segments of code to be similar to the ones used by those countries in the past, established a connection to governmental infrastructure, or some combination thereof.[150]

Riesland will counter that cyber security technologists and computer scientists have criticized the FBI's approach towards attribution.[151] Indeed, Riesland may direct the Court to the standards espoused in the Tallinn Manual as a better reflection of the current state of the law.[152] There, in Rule 7, the Group of Experts makes it explicitly clear that though "the fact that a cyber operation has been mounted from government cyber infrastructure is an indication of that State's involvement," it "in and of itself [...] does not serve as a legal basis for taking any action against the State involved or otherwise holding it responsible for the acts in question."[153] Similarly, in the context of IP routing and trace-backs, the Manual specifies that "the mere passage of data through the infrastructure located in the State does not presuppose any involvement by that State in the associated cyber operation."[154] The Manual explains this approach as a safeguard against incorrect attribution, as the nature of Internet spoofing, as above discussed, renders even governmental networks susceptible to hacks by unaffiliated third parties.[155] For this reason the Court should uphold the higher threshold of "reasonable certainty" in attribution adopted by the ILC, and deem the circumstantial evidence provided by Amestonia as insufficient in meeting that bar for direct attribution.

Judges should note that neither of these two approaches are matters of settled law. Judges are encouraged to ask students for specific reasons as to why one standard or another should be adopted.

2. Riesland's Liability Under Standards of Due Diligence

a. The Doctrine of "Due Diligence" in International Law

---

[150] *See e.g.*, Ellen Nakashima, *U.S. Attributes cyberattack on Sony to North Korea*, The Washington Post (19 December 2014), *available at* https://goo.gl/TBO4BD.

[151] *See e.g.*, Marc Rogers, *No, North Korea Didn't Hack Sony*, The Daily Beast (24 December 2014), *available at* http://goo.gl/Qu2mky; Robert Graham, *The FBI's North Korea Evidence is Nonsense*, Errata Security Blog (19 December 2014), *available at* http://goo.gl/lxyThV; Kim Zetter, *Critics Say New Evidence Linking North Korea to the Sony Hack is Still Flimsy*, WIRED (8 January 2015), *available at* http://goo.gl/GHpQrl.

[152] In 2009, the NATO Cooperative Cyber Defense Centre of Excellence, an international military organization based in Tallinn, Estonia, invited an independent international group of experts to produce a manual on the law governing cyber warfare. The project brought together distinguished international law practitioners and scholars in an effort to examine the extant legal norms applied to this 'new' form of warfare. The *Tallinn Manual 1.0* was first published in 2013 and was directed by Prof. Michael Schmitt of the United States Naval War College. While the final document is described as "non-binding", it is considered to date to be the most reputable and authoritative analysis of currently existing law as it applies to cyber warfare (it can be examined as a subsidiary means for the determination of the rules of international law, under ICJ Statute Article 38(1)(d) as it reflects the teaching of the most highly qualified publicists). Tallinn Manual 1.0 focused on the type of cyber attacks that constitute a "use of force" under U.N. Charter Art. 2(4) or form part of a broader offensive campaign within the context of an armed conflict as governed under international humanitarian law and the Geneva Conventions.

[153] Tallinn Manual, *supra* note 140., at 35.

[154] *Id.*, at 36.

[155] *Id.*, at 35-36.

The legal maxim of *Sic Utere Tuo Ut Alienum Non Laedas* ("use your own property as not to harm that of another") is directly tied to the principle of good neighborliness enshrined in Article 74 of the U.N. Charter. Recognized by the ICJ in the *Corfu Channel* case as "a general and well-recognized principle of international law,"[156] it imposes an obligation on a State not to knowingly allow its territory to be used for acts contrary to the rights of other States. This duty not to harm has been given many names over the years, including the principle of prevention, principle of precaution, and States' broader "due diligence" obligations. It follows from all of these that States must adopt any necessary measures in order to avoid or reduce damage beyond its own territory, and to inform, notify, consult, and share information with its neighbors on situations involving transboundary harms.[157]

The question becomes whether violations of due diligence obligations (or the doctrine of *Sic Utere Tuo*), constitute only violations of primary obligations,[158] or whether they qualify as secondary rules thereby triggering State Responsibility of the entire wrongful act. Note that the ILC in its draft articles refrained from answering the question.[159] The International Tribunal for the Law of the Sea took a similar approach, noting that "due diligence is a variable concept" and that the standard may change as a result of technological developments as well as the potential risks involved in each activity.[160]

b. Applying "Due Diligence" in the Cyber context

The United States President, in his International Strategy for CyberSecurity of May 2011, has identified the standard of due diligence as an "emerging norm" in the cyber sphere, suggesting that "states should recognize and act on *their responsibility* to protect information infrastructures and secure national systems from damage or misuse (emphasis added)."[161] Some scholarly writings assert that cyber

---

[156] *See* Corfu Channel, *supra* note 8, at p. 22.

[157] For a complete analysis, *see* Katharina Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 135, 165-171 (Katharina Ziolkowski ed., 2013). *See also*, International Law Commission, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, UN Doc A/56/10 (2001). As James Crawford had noted: "despite the uncertainty surrounding their future status, the Draft Articles [on Prevention of Transboundary Harm] provide an authoritative statement of the scope of a state's international legal obligation to prevent a risk of a transboundary harm." JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY 82 (2002).

[158] As was the case for example in *Trail Smelter* where it was determined that given Canada's capacity to limit transboundary damage, by improving emissions control technologies, it failed to meet its due diligence obligations. *See*, Trail Smelter Case (United States v. Canada), U.N. Reports of International Arbitral Awards, Vol. III pp. 1905-1982 (16 April 1938, 11 March 1941).

[159] ILC Articles on State Responsibility, *supra* note 22, at 34. The ILC noted that: "Whether responsibility is "objective" or "subjective" in this sense depends on the circumstances, including the content of the primary obligation in question. The articles lay down no general rule in that regard. The same is true of other standards, whether they involve some degree of fault, culpability, negligence or want of due diligence. Such standards vary from one context to another for reasons which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation."

[160] Responsibilities and Obligations of States Sponsoring Persons with Respect to Activities in the Area, Advisory Opinion, ITLOS Sea Bed Disputes Chamber Reports, Case no. 17, ¶ 117 (1 February 2011).

[161] President of the United States, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011), *available at* https://goo.gl/Gzhx8u.

security 'due diligence' is already part of international custom.[162] The U.N. Group of Governmental Experts, in their report to the U.N. Secretary General in July 2015, took a slightly more nuanced approach. The UNGGE considered the "challenges of attribution in the [cyber] environment," and suggested, as a matter of non-binding responsible behavior, that States should not "knowingly allow their territory to be used for internationally wrongful acts using [cyber means]."[163]

In the present case, Amestonia will contend that Riesland had a due diligence obligation to ensure that either its information infrastructures, or at the very least, its own governmental infrastructures, were not being used to launch an attack. In *Corfu Channel*, the ICJ ruled that since Albania's lookout posts were within sight of the minefield location, Albanian authorities must have had knowledge of the existence of the mines and their locations. Thus, Albania was indirectly held responsible for not providing prior notification to the British warships.[164] Here, Riesland is a technologically advanced country with a rapidly expanding IT sector. It arguably had the capacity to closely monitor its governmental cyber infrastructures, in the same manner that Albania monitored the Corfu strait. This capacity forms the basis for establishing its constructive knowledge of the attack. By knowingly failing to prevent the attack *ex ante*, Riesland should be held liable for the consequences of the attack *ex post*. Furthermore, failing to provide *ex post* assistance and information in identifying the perpetrators of the attack should also be considered in analyzing Riesland's overall culpability.

Riesland will counter that "due diligence" obligations in cyber sphere have not yet risen to the level of a customary obligation binding on Riesland as such but, rather, can be said to be a non-binding best practice at best. Riesland will further note that even if it was bound by due diligence requirements, such requirements are applicable only as primary obligations, but cannot serve as the basis for attribution of the cyber attack itself. From a practical standpoint, Riesland may note that it is technologically impossible in this modern age to ensure the absolute prevention of a country's information infrastructures from being hacked and exploited; therefore, establishing such an extreme standard of attribution will be unreasonably burdensome.

B. Did the Cyber Attack Constituted an Internationally Wrongful Act

1. Violation of the Prohibition on the Use of Force

Amestonia may argue that the cyber attack against the *Ames Post* and Chester & Walsingham constituted a use of force, in violation of Article 2(4) of the U.N. Charter. In accordance with Rule 11 of the Tallinn Manual and the ICJ's broader jurisprudence in *Nicaragua*,[165] Amestonia will have to show that that the cyber attack's "scale and effects are comparable to non-cyber operations rising to the level of a use of force."[166] The Tallinn Manual notes that a contextual analysis is required, one which

---

[162] Katharina Ziolkowski, *supra* note 157, at 168.

[163] United Nations Group of Governmental Experts Report on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174, p. 7, ¶ 13 (22 July 2015) (hereinafter: 2015 UNGGE Report).

[164] Corfu Channel, *supra* note 8, at pp. 21-22.

[165] Nicaragua, *supra* note 23, at ¶ 195.

[166] Tallinn Manual, *supra* note 140, at 45.

examines, *inter alia*, the severity of the attack, the measurability of its effects, its invasiveness, and its military character.[167]

Amestonia may focus on the significant economic damages from the attack (estimated at €45-50 million) coupled with the harms caused to Amestonian society (the shutting down of its "most widely-circulated" newspaper for three months, and the significant disruption to Amestonia's judicial system involving the law firm) as justifying deeming the attack a "use of force." Amestonia may claim further that an effective judiciary and media form part of a country's critical infrastructures, which receive heightened protections in cyber law.[168] However, as one commentator has noted, traditional understanding of "use of force" involves "armed force" requiring Amestonia to show "kinetic effects of a physical nature on a body or on an object."[169] Thus, Riesland would contend – in a way that is more in line with the current state of the law – that any delay or interruption in the transfer of data, including any manipulation, suppression, or deletion of such data, especially when the target is a private corporate non-military target, cannot be deemed to meet the necessary bar to qualify as a use of force. Such attacks would seem to fall below the ambit of the U.N. Charter prohibition.[170] **Judges are generally encouraged to move students away from lengthy use of force arguments.**

2. Violation of Territorial Integrity and the Principle of Non-Intervention

The aspect of territorial sovereignty, *i.e.*, the exercise of full and exclusive authority over a territory, protects physical components of the Internet and cyber infrastructures that are located on a State's territory or are otherwise under its exclusive jurisdiction. As the Tallinn Manual clarifies in Rule 1 on Sovereignty: "A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty." The manual goes even further and says that "it will certainly do so" in cases where malware causes physical damage.[171] Amestonia will contend that the above-mentioned economic and social effects constituted such "physical damage." Alternatively, Amestonia will argue in line with expressed U.S. positions that "due to the enormous negative effects malicious cyber activities have on the national security of another State," physical damage should no longer be the applicable standard.[172] Indeed, any kind of "disruption of networks and systems" should constitute a violation of sovereignty.[173] Riesland will contend that any violation of territorial integrity requires some form of "physical damage" beyond the mere deletion of data.

Either alternatively, or cumulatively, Amestonia may argue that the attack took place only 8 days after the decision of President Hale not to extradite Frost or seize the documents Frost stole. The attack should therefore be deemed an action of political interference by Riesland in the domestic affairs of

---

[167] *Id.*, at 48-52.

[168] 2015 UNGGE Report, *supra* note163, at 13(g).

[169] Katharina Ziolkowski, *supra* note 157, at 173.

[170] *Id.*

[171] Tallinn Manual, *supra* note 140, at 16-17.

[172] Katharina Ziolkowski, *supra* note 157, at 163.

[173] President of the United States, International Strategy for Cyberspace, *supra* note 161, at 4.

Amestonia. Riesland attempted to self-enforce its positions and penalize *The Ames Post*, Chester & Walsingham, and, indirectly, Amestonia *writ large*. This kind of activity will be argued to be seen as reaching the level of coercive intervention, violating the obligations laid out in Article 2(7) of the Charter. Riesland may counter that the cyber attack fell short of coercion as it was not intrusive enough to affect Amestonian domestic affairs since the targets were the computer system of two private entities. Riesland may further claim "necessity" as a circumstance precluding wrongfulness.[174]

3. Violation of Freedom of Expression

Article 19 of the Universal Declaration and Article 19 of the ICCPR protect the right "to seek" and "impart" information and ideas as an integral aspect of the right to freedom of expression. In its case law, the ECtHR has made clear that the European Convention's strong protection of freedom of expression rests in significant measure on the public's right to know. For instance, in referring to the special protection to be accorded to the press, the ECtHR has repeatedly stated: "Not only does the press have the task of imparting such information and ideas [on matters of public interest]: the public also has a right to receive them. Were it otherwise, the press would be unable to play its vital role of "public watchdog."[175] The public's right to know is also an intrinsic aspect of informed political debate crucial to genuine democracy. Indeed, "freedom of the press affords the public one of the best means of discovering and forming an opinion of the ideas and attitudes of political leaders. More generally, freedom of political debate is at the very core of the concept of a democratic society[.]"[176] The ECtHR has further ruled that the right to receive information "basically prohibits a Government from restricting a person from receiving information that others may wish or may be willing to impart to him."[177]

When Governments decide to shut down newspapers for political reasons -- for example, in the context of the closure of the Basque newspaper Egunkaria in Spain, the Daily News in Zimbabwe (Harare), or the Haatuf newspaper in Somaliland – they have been sharply criticized for potential abuses of ICCPR Article 19.[178] In the present case, Riesland may be said to have effectively shut down the *Ames Post* for three months. Riesland may again contend that the ICCPR is not applicable extraterritorially, or that it was required to take the action it did on grounds of necessity, given the threat the newspaper leaks posed to Riesland's national security. It may further argue that the attack was aimed at the deletion of the data, not the shutting down of the newspaper.

4. Violation of Attorney-Client Privilege

The hacking of the computer systems of Chester & Walsingham had negative effects on both the law firm's ability to represent Frederico Frost, as well as many of its other clients. What is often termed

---

[174] For a specific analysis of coercion and unlawful intervention arguments in the cyber attack context *see* Katharina Ziolkowski, *supra* note 157 at 164-165; Tallinn Manual, *supra* note 140, at 44-45.

[175] *See, e.g.*, The Sunday Times v United Kingdom (No. 2), App. No. 13166/87, ¶ 50 (24 October 1991).

[176] Lingens v Austria, 8 EHRR 407, ¶ 42 (8 July 1986).

[177] Leander v Sweden, App no 9248/81, 9 EHRR 433, ¶ 74 (26 March 1987).

[178] For example, the International Commission of Jurists has sharply criticized the closure of Egunkaria in its submission before the Human Rights Committee as a violation of Article 19. See *Human Rights Committee Consideration of the Fifth Periodic Report of Spain – Submission on List of Issues*, International Commission of Jurists (2009) at page 8.

"legal professional privilege" in domestic legal systems may be seen as a customary or general principle of law within the meaning of Article 38(1)(c) of the ICJ Statute. Indeed, most States recognize some form of attorney-client privilege to protect the professional secrecy of confidential communications between legal advisers and their clients. The principle is fundamental to the international rule of law.[179]

In *Questions Relating to the Seizure and Detention of Certain Documents and Data*, the ICJ recognized that States have a right to communicate with their counsel and a derivative right to the protection of their communications with counsel, including the confidentiality of correspondence and other data prepared by counsel, and relating to an arbitration or to negotiations. The ICJ derived its conclusion from the U.N. Charter principles of sovereign equality fundamental to our legal order.[180] Amestonia may attempt to argue that the same protections under international law are granted not only to States but also to individuals. It may try to establish this protection from the right of due process protected under Article 14 to the ICCPR.

5. Other Possible International Legal Obligations

As they continue work on Tallinn Manual 2.0, NATO's Group of Experts is examining various legal fields to identify potential violations of international law that can be caused by low-intensity, one-off, cyber attacks. Students are encouraged to follow this initiative, in an effort to identify other potential violations. Judges should also embrace creative arguments that go outside the bounds of this bench memorandum, so long as they are persuasive, rely on substantive rules of law, and are logically structured. In this sense, we expect that some teams may make arguments relating to international telecommunication law (in particular, arguments relating to the Constitution of the International Telecommunications Union),[181] arguments relating to States' obligations to peacefully settle disputes under U.N. Charter Article 33; arguments relating to violations of due diligence as a primary obligation; and arguments relating to States' obligations to protect the property rights of foreign individuals.

---

[179] Questions Relating to the Seizure and Detention of Certain Documents and Data, Timor Leste v. Australia, I.C.J Reports 2014, Memorial of the Democratic Republic of Timor-Leste, 52 (28 April 2014).

[180] *Id.*, Request for the Indication of Provisional Measures, Order, I.C.J Reports 2014, p. 147, at ¶ 27 (3 March 2014).

[181] Article 34 of the Constitution reserves the right of Member States to "stop in accordance with their national law, the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its laws, to public order or decency..."

Note that some teams under QP1 could raise Articles 37 and 38 of the Constitution, which are titled "Secrecy of Telecommunications", and Establishment, Operation, and Protection of Telecommunication Channels and Installations, respectively. Article 37 reads: (1) Member States agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence; (2) Nevertheless, they reserve the right to communicate such correspondence to their competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are parties. Article 38 reads in relevant part: (3) Member States shall safeguard these channels and installations; (4) Unless other conditions are laid down by special arrangements, each Member State shall take such steps as may be necessary to ensure maintenance of those sections of international telecommunication circuits within its control; (5) Member States recognize the necessity of taking practical measures to prevent the operation of electrical apparatus and installations of all kinds from disrupting the operation of telecommunication installations within the jurisdiction of other Member States.

Appendix A: Introduction to International Law

This section is a primer on public international law for judges who may not have professional experience or training in the field. There is an important distinction between international law and most domestic legal systems in terms of what sources of law are acceptable before the Court.

A. General

The Statute of the Court governs the conduct and rules of the International Court of Justice (ICJ). Under Article 38(1) of the ICJ Statute, the ICJ may consider the following sources of international law in order to decide disputes before it:

(a) treaties or conventions to which the contesting States are parties;

(b) international custom, as evidence of a general practice accepted as law;

(c) general principles of law recognized by civilized nations;

(d) judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

Commentators disagree as to whether the first three sources are listed in order of importance. All of these sources are perfectly acceptable before the Court and an important aspect of argumentation before the ICJ includes advocating for why a particular source is more or less relevant than another source.

Judges from common-law systems should note the status of precedent. Article 59 of the ICJ Statute states that decisions of the Court are binding *only on the parties to the case*, and are without formal effect as precedent. However, in practice, the ICJ often cites both its prior decisions and those of its predecessor, the Permanent Court of International Justice, as persuasive authority (pursuant to Article 38(1)(d)). Additionally, the Court frequently evaluates rules of customary international law in its opinions and subsequently relies upon those evaluations.

Resolutions of the United Nations General Assembly are not, of themselves, binding upon the Court. Resolutions can be argued to reflect evidence of state opinion on an issue, evidence of a general principle, or even as a reflection of state practice or *opinio juris* to help establish custom.

B. Treaties

Treaties are agreements between and among States, by which parties obligate themselves to act according to the terms of the treaty. Rules regarding treaty procedure and interpretation are defined in the Vienna Convention on the Law of Treaties (VCLT).

Article 26 of the VCLT sets out the fundamental principle relating to treaties, *pacta sunt servanda*, which provides that "every treaty in force is binding upon the parties to it and must be performed by them in good faith." Even if a State is not party to a treaty, the treaty may serve as evidence of customary international law if, over time, its provisions have come to be regarded as custom by nonparty states. Judges should be aware, however, of instances where a treaty might not be custom in its entirety, but some of its provisions may very well have ascended to the level of custom.

Article 31 of the VCLT requires that treaties be interpreted in good faith, in accordance with its ordinary meaning given its context, and in light of its object and purpose. The context of a treaty can be taken from a variety of sources including a treaty's preamble or annexes, any prior or subsequent agreements between the parties related to the treaty, and any relevant rules of international law. If the meaning is

still ambiguous, one may also take into account supplementary methods of interpretation, including references to the *travaux preparatoires* (akin to legislative history) of the treaty and the circumstances of its conclusion.

C. Customary International Law

The second source of international law is customary international law (also known as "custom"). A rule of customary international law is one that has binding force of law because the community of states treats it and views it as a rule of law. In contrast to treaty law, a rule of customary international law is binding upon a state whether or not it has affirmatively assented to that rule.

In order to prove that a given rule has become custom, one must prove two elements: widespread state practice and *opinio juris*. "State practice" refers to a sufficient number of states behaving in a regular and repeated manner consistent with the argued for rule of custom. Some commentators argue that the practice of a small number of states in a particularized region can create "regional customary international law." Others argue that the practice of specially affected states (such as in the area of space law where there few state participants) can create custom that binds other non-specially affected states as long as those states acquiesce to the practice of the specially affected states. The ICJ has acknowledged both of these possibilities.

Opinio juris is the subjective element of customary international law. It requires that the state action in question is done out of a belief that the rule is law. Put another way, *opinio juris*, is the "conviction of a State that it is following a certain practice as a matter of law and that, were it to depart from the practice, some form of sanction would, or ought to, fall on it." MARK E. VILLIGER, CUSTOMARY INTERNATIONAL LAW AND TREATIES 4 (1985).

Customary international law is shown by reference to treaties, decisions of national and international courts, national legislation, diplomatic correspondence, opinions of national legal advisers, and the practice of international organizations. Each of these items might be employed as evidence of state practice, *opinio juris*, or both. In the *North Sea Continental Shelf Cases*, the ICJ stated that the party asserting a rule of customary international law bears the burden of proving it meets both requirements.

D. General Principles of Law

The third source of international law consists of "general principles of law." The bulk of recognized general principles are procedural in nature (e.g., burden of proof and admissibility of evidence). Many others, such as waiver, estoppel, unclean hands, necessity, and *force majeure*, may sound familiar to a common-law practitioner as doctrines of equity. The principle of general equity in the interpretation of legal documents and relationships is one of the most widely cited general principles of international law.

It is important to note, however, that "equity" in this sense differs from the Court's power to decide a case *ex aequo et bono* (considering solely principles of "right and wrong"), a separate matter treated under Article 38(2) of the Statute.

E. Subsidiary Means of Finding the Law

The final sources of international law are "a subsidiary means of finding the law" which often include judicial decisions and scholarly writings. These act, essentially, as research aids for the Court, and are often used to support or refute the existence of a customary norm, to clarify the bounds of a general principle or customary rule, or to demonstrate state practice under a treaty.

Judicial decisions, whether from international tribunals or from domestic courts, are useful to the extent that they address international law directly, demonstrate a general principle, or remark upon a similar situation to the case at hand.

Many student competitors make the mistake of believing that any published article rises to the level of an Article 38(1)(d) "teaching." This provision is limited to the teachings of "the most highly qualified publicists." For international law this can includes names such as Grotius, Lauterpacht, Oppenheim, McNair and Brownlie. This list is NOT exclusive and judges should question oralists about the identity and validity of a cited scholarly source. Furthermore, authoritative sources within this list can include the writings of former Judges, the secondary opinions of Judges who decline to join the majority in a case, and documents created by the International Law Commission (ILC). Within the context of a specific field, there are additional scholars who could also be regarded as "highly qualified publicists."

F. Burdens of Proof

In the *Corfu Channel Case* (*U.K. v. Albania*, 1949), the ICJ set out the burdens of proof applicable to cases before it. The Applicant normally carries the burden of proof with respect to factual allegations contained in its claim and must satisfy this burden via a preponderance of the evidence. The burden falls on the Respondent with respect to factual allegations contained in a cross-claim. The Court may also draw an adverse inference against a party if it refuses to produce evidence that is solely within its own control.

Appendix B: Timeline of Events

1967 - The Secret Service Bureau Act is adopted and the Bureau is established.

11 December 1970 - Famed Rieslandic state visit to Amestonia that begins an era of closer economic ties between the two countries. A number of Bilateral Agreements are signed including in the fields of extradition and intelligence sharing.

1992 - Amestonia and Riesland establish a free trade area in agriculture and agriculture related goods.

4 March 1992 - Amestonia and Riesland sign the Treaty on the Establishment of Broadcasting Facilities ("the Broadcasting Treaty")

22 December 1992 - The inaugural program of the Voice of Riesland (VoR) and its Amestonian counterpart airs.

Early 1990s – The Institute for Land and Sustainable Agriculture (ILSA) begins raising concerns about the long term effects of Amestonian farmers' reliance on neonicotinoids, produced in Riesland, to boost yields.

1998 - Riesland becomes the top importer of Amestonian agricultural produce.

2003 - The Terrorism Act is enacted in Riesland.

2003-2013 - Between these years Amestonia saw an annual GDP growth rate of between 6.8% and 7.4%, the highest in the region.

2 October 2012 - ILSA publishes the report, "The Plight of the Bumblebee", which examined the negative effects of the increased use of neonicitonoids on the regional bee population. ILSA urged the two countries to reevaluate their production and use of neonicotinoids.

May 2013 - The Bureau installs a waterproof recording pod on the primary backbone of Amestonia's international Internet and telephone communications traffic. The operation is code-named "Verismo".

24 May 2013 - The European Commission adopts restrictive regulations on neonicotinoids, sparking academic and parliamentary debates within Amestonia and Riesland on the issue. Neither government takes any action.

2 July 2013 - www.longlivethehive.com launches, inviting environmental activists to use its anonymous forums and chat rooms to discuss ways to stop the continued production and use of neonicitonoids.

2 February 2014 - Seven Amestonian warehouses, containing a significant number of barrels of neonicitonoids, are set on fire. The fires cause five deaths, including two Rieslandic nationals. Police found a spray-painted image of a bee on the asphalt outside each of the warehouses.

3 February 2014 - Amestonian President, Jonathan Hale is a guest on VoR's most popular news show, "Tea Time with Margaret," where he speaks out against the warehouse fires.

7 March 2014 - 263 Envelopes, containing a non-toxic variant of neonicotinoid and stamped with the image of a bee, are mailed to government and business figures in Amestonia and Riesland with connection to neonicotinoid policies. Later, an anonymous tweet warns that next time the envelopes will be poisoned.

8 March 2014 - Riesland's Prime Minister, Alice Silk, and President Hale discuss the attacks. Riesland offers cooperation, including the sharing of intelligence. Silk subsequently orders Riesland's security and intelligence services to direct their operations against the new threat of "eco-terrorism".

2 July 2014 - The Office of James Deloponte, the Attorney General of Riesland, issues internal regulations regarding intelligence collected via the Verismo Program and other related operations.

16 October 2014 - The Bureau's director, Tom Sivaneta, meets with the Amestonian Minister of Internal Affairs and informs him of a ring of Amestonian activists plotting to infect a large shipment of honey intended for Rieslandic consumption.

17 October 2014 - Riesland declares a Terrorism Alert pursuant to the Terrorism Act.

21 October 2014 - Amestonian police arrest a group of college students who were planning an attack on a number of honey extraction facilities. The students admit that they are affiliated with a group of environmentalists known as "The Hive".

16 December 2014 - Frederico Frost, a Bureau intelligence analyst, leaves Riesland with a USB drive containing 100,000 documents labeled "top secret". Chester & Walsingham, an Amestonian law firm, agrees to represent Frost in relation to any disclosure of the materials.

18 December 2014 - Frost meets with reporters from *The Ames Post* and requests that the newspaper publish the content of the documents on its website.

Jan-Feb 2015 - *The Ames Post* publishes a series of reports relaying information from Frost's files.

23 January 2015 - *The Ames Post* publishes a document entitled: "The Verismo Program" on its website, revealing the scope and reach of Riesland's mass surveillance against Amestonian nationals.

29 January 2015 - *The Ames Post* reveals that on least 50 different occasions Amestonia had received redacted information related to terrorist activity obtained via the Verismo Program.

2 February 2015 - Riesland's Foreign Ministry sends a note to Amestonia requesting the immediate extradition of Frost and the recovery of all information stolen by Frost.

16 February 2015 - *The Ames Post* releases another Bureau document revealing that since its inception the VoR station has been used to collect intelligence on Amestonian public figures. That night, an emergency warrant is granted to seize the assets and property of VoR. While police are applying for the warrant, VoR's broadcasting is interrupted. Upon execution of the warrant Amestonian police find nothing but an empty studio, save for the broadcasting equipment.

17 February 2015 - Mayer and two other VoR employees are caught on board a train at the Amestonian border, attempting to leave for Riesland. In the aftermath, President Hale holds press a conference criticizing Riesland and the scope of its spying, and defending the seizure of VoR and arrest of Mayer.

19 February 2015 - Prime Minister Silk holds a televised interview, where she rejects Hale's statement, defends Riesland's programs, and accuses Amestonia of harboring Frost.

7 March 2015 - Joseph Kafker, a retired Amestonian Green Party politician, is detained in Riesland in accordance with the Terrorism Act, after giving the keynote address at a conference.

8 March 2015 - The Amestonian Parliament holds a Special Session denouncing Kafker's detention and demanding his release. Riesland does not respond.

10 March 2015 - Kafker appears before Riesland's National Security Tribunal and his detention is upheld. The tribunal grants a petition to extend Kafker's detention for reasons of national security, and further rules that all evidence pertaining to Kafker's apprehension is to be considered "closed material".

12 March 2015 - Amestonia's Foreign Minister demands access to the evidence against Kafker, and criticizes the Terrorism Act's compliance with human rights standards. Riesland rejects the request claiming that the National Security Tribunal has prevented the release of this information.

14 March 2015 - Amestonia officially refuses to extradite Frost, citing the "political offence" exception. It further denies the request for the documents stolen by Frost. Riesland's Attorney General responds in a statement noting that Riesland will do whatever in its power to prevent further leaks.

17 March 2015 - *The Ames Post* reveals, through another leaked document, that Kafker was hacked while a guest on "Tea Time With Margaret." Attorney General Deloponte states that Riesland was in possession of "closed materials" that "directly link Kafker to the Hive's senior echelons."

22 March 2015 – The computer systems at Chester & Walsingham and *The Ames Post* are hacked and disabled to the extent that nearly 90% of their information is "non-recoverable". Total damages are estimated €45-50 million.

April 2015 - Riesland reissues a second Terrorism Alert.

1 April 2015 - President Hale denounces the cyber attack.

5 April 2015 - Attorney General Deloponte refuses to respond to allegations that Riesland was involved in the attack.

6 April 2015 - Divers from the German Telecommunications company, which owns the undersea fiber optic cable tapped by the Bureau, are sent to dismantle the pod. Upon doing so they determine that it did not cause any breaking or injury to the cable, nor did it interrupt or in any other manner obstruct communications.

22 April 2015 - Amestonia concludes its investigation into VoR and determines that a number of items found in the station were used for surveillance. Amestonia's government obtains a forfeiture order and expresses its intentions to sell the station's real estate and property by means of a public auction. All

challenges by attorneys from Riesland's National Television Corporation (VoR's mother organization) are rejected and subsequent appeals are dismissed within Amestonia's courts.

Mid-2015 - Both nations begin at attempts to settle all outstanding issues and grievances.

July 2015 - Amestonia circles a resolution around the Human Rights Committee asking for the Special Rapporteur to determine the legality of Riesland's programs.

7 July 2015 - *The Sydney Morning Herald* publishes a report alleging that Riesland's supporters on the Human Rights Council have encouraged it to settle its dispute with Amestonia, expressing concerns about their ability to continue to share intelligence with Riesland without fear of being complicit in human rights abuses.

October 2015 - Riesland issues a third Terrorism alert.

Appendix C: Guide to People, Places, and Acronyms

@buzzkiller24601
Twitter account of an associate of the Hive

Alice Silk
Prime Minister of Riesland

Amestonia
A developing agricultural country, the Applicant

Amestonian Institute of Technology (AIT)
World-renowned academic institution with a focus on engineering and computer science

The Ames Post
Leading national newspaper of Amestonia that was subjected to a cyber attack

Blaster
A rootkit malware used in the Carmen program.

The Broadcasting Treaty
Treaty for the Establishment of Broadcasting Facilities signed by the Countries in 1992

The Bureau
Rieslandic agency that engages in intelligence collection pursuant to the provisions of the SSBA

The Carmen Program
A Bureau operation to collect intelligence on top Amestonian public figures, located inside VoR

Chester &Walsingham
Law firm who represented Frederico Frost and was subjected to a cyber attack

David Cornwell
Amestonia's ambassador to the United Nations; one of the targets of the Carmen program.

Frederico Frost
Bureau analyst turned Whistleblower who leaked 100,000 Rieslandic confidential documents

The Hive
Eco terrorist group linked to planned attacks in Amestonia and Riesland

ICJ
The International Court of Justice

Institute for Land and Sustainable Agriculture (ILSA)
Dutch NGO monitoring regional biodiversity.

James Deloponte
Attorney General of Riesland

Jonathan Hale
President of Amestonia

Joseph Kafker
Retired Amestonian politician currently under preventative detention within Riesland

Margaret Mayer
Head of VoR, a Rieslandic television icon who was involved in the Carmen Program

National Security Tribunal
A Rieslandic court with intelligence and detention oversight capacities established under the SSBA

Neonicotinoids (Neonics)
A class of neuro-active insecticides produced by Rieslandic companies to boost yields in Amestonia

The Opera House
Code name for an underground floor within the VoR where intelligence was stored and analyzed

Riesland
A developed democratic state, the Respondent

Riesland National Television
A State-owned and operated corporation; VoR is one of its divisions.

SSBA
Secret Surveillance Bureau Act adopted in 1976 and established the mandate of the Bureau.

Tom Sivaneta
Current director of the Bureau; authorized the Verismo program.

The Verismo Program
A mass surveillance program which tapped an Amestonian underwater cable.

Voice of Riesland (VoR)
Division of Riesland National Television, established under the Broadcasting Treaty.

Appendix D: Issue Spotter for Judges

This appendix is a summary of the bench memorandum. It aims to assist judges by providing them with an abridged outline of the main legal arguments surrounding the case. Every argument listed below is accompanied by a correlating page number within the bench memorandum, for further reading.

QP1

1. Are The Ames Post documents admissible before the ICJ? (pp.7-9)

A: In the practice of both the PCIJ and ICJ evidence "is seldom excluded." (*p.7*)

In line with *Corfu* evidence wrongly acquired might still be relied on. (*p.8*)

Ex Injuria is inapplicable as Amestonia is not the wrongdoer, but a third party beneficiary. (*p.8*)

crimen omnia ex se nata vitiat has not risen to the level of a general principle of int'l law. (*p.8*)

The documents are *prima facie* reliable, authentic and of probative value (*Wikileaks* case). (*p.9*)

Relying on published materials does not endanger Riesland's national security. (*p.9*)

R: "Property obtained by crime is vitiated" (*crimen omnia ex se nata vitiat*). (*p.8*)

"Law does not arise from injustice" (ex injuria jus non oritur). (*p.8*)

By analogy, classified documents may be excluded in arbitration proceedings (IBA Rules). (*p.9*)

The Court will legitimize the stealing and leaking of government confidential documents. (*p.9*)

2. Did Riesland's surveillance programs violate international law? (pp.9-15)

A: The programs breached territorial sovereignty and non-intervention (*Can. Fed. C.*). (*p.9*).

Amestonia did not acquiesce to the programs, as it was unaware of their scope and reach. (*p.9*)

In line with the HRC and UNGA, ICCPR applies extraterritorially in surveillance cases. (*p.12*)

Riesland breached Art.17 to the ICCPR on the Right to Privacy (*e.g. Zakhrov v. Russia*). (*p.13*)

Riesland abused its right to collect intelligence for counter-terrorism purposes. (*p.14*)

Verismo violated Riesland's "due regard" and "lawful uses" obligations within its EEZ. (*p.15*)

Carmen violated Riesland's obligations on the inviolability of diplomatic correspondence. (*p.15*)

R: There exist no prohibition on peacetime espionage, and in line with *Lotus* it is lawful. (*p.9*)

Monitoring of cables does not interfere with territorial sovereignty (Germany in *Weber*). (*p.10*)

Intelligence produced from the programs benefited Amestonia, which consented to them. (*p.10*)

The ICCPR is inapplicable and in any event the programs did not violate Article 17. (*pp..12-14*))

Riesland has a right and an obligation to collect intelligence to counter terrorism. (*p.14*))

Verismo was in accordance with Riesland's rights and obligations under Customary LOS. (*p.15*)

Spying on public figures and diplomats is accepted practice in international affairs. (*pp.11, 15*)

3. Should the Court order cessation with assurances of non-repetition? (pp. 15-16)

A: In line with *Chorzow* and *Nicaragua* the Court may declare such a remedy. (*p.16*)

R: Both Verismo and Carmen have effectively ceased and are not a "continuing wrong." (*p.16*)

The Court may not determine the legality of future programs, which will have to be examined on the basis of their individual merits, and therefore cannot demand such assurances. (p.16)

QP2

1. Did the seizure of the VoR's assets and the arrest of its employees violated the BT? (pp. 17-20)

A: All Immunities cease to have effect upon the cessation of VoR's functions (BT Art. 36). (*p.17*)

The abandonment of the station and interruption in broadcasting, should be interpreted as the effective "cessation of functions." (*p.18*)

Entering the Station was lawful given the immediate threat to public safety posed by Riesland's surveillance activity (BT Art. 14(1)). (*p.18*)

The VoR employees' immunities do not continue to subsist as any spying activity cannot be deemed as "acts performed in the exercise of the station's functions" (BT Art. 15(1)(c)). (*p.18*)

The BT is the *lex specialis* and it does not include a *persona non grata* clause. (*p.19*)

R: The warrant, which was sought before the interruption in broadcasting, violated the BT. (*p.18*)

At all times the Stations continued to fulfill its functions as content was still being aired. (*p.18*)

The temporary abandonment of the Station is justified given Amestonia's failure to protect the VoR Station and its employees (BT Art. 14(2)). (*p.18*)

Certain immunities should continue to subsist regardless of cessation of functions: namely inviolability of archives and immunities of employees (BT Art. 14(4), Art. 15(1)(C)). (*p.18*)

Riesland should have expelled the VoR employees in accordance with the customary practice of *persona non grata* declarations. (*p.19*)

2. Was the BT valid and in force during the seizure/arrest, and May Riesland invoke it? (pp. 20-22)

A: The BT is invalidated as Amestonia was deceived during negotiations (VCLT Art. 49). (*p.20*)

By engaging in spying activities, Riesland violated BT Art. 23, and that violation constitutes a material breach justifying termination of the treaty. (*p.21*)

Riesland may not invoke the BT before the ICJ as it comes with unclean hands. (*p.22*)

Amestonia's actions were necessary and their wrongfulness precluded (ILC Art. 25). (*p.22*)

R: There is no evidence of any false statements during negotiations to establish fraud. (*p.21*)

The wording "without prejudice" in BT Art. 23 establishes that the parties never intended for breaches of this article to be deemed material. (*p.21*)

"Clean Hands" remains unsettled in international law and has rarely been applied. (*p.22*)

The surveillance activity is not a "grave and imminent peril" justifying a preclusion of wrongfulness under grounds of necessity (ILC Art. 25). (*p.22*)

3. Did the station's seizure and arrest of its employees violate Riesland's state immunity? (pp. 23-24)

A: VoR is a branch of RNT, a Riesland state-owned and operated corporations. (*pp.23-24*)

Because of both the nature of TV broadcasting and Carmen's economic espionage, VoR served commercial purposes, excluding Riesland from invoking jurisdictional immunities. (*p.23*)

In accordance with Article 15 of the UN Convention on Jurisdictional Immunities Riesland may not invoke its immunity in proceedings that relate to its participation in a company located in Amestonia. (*p.24*)

Amestonia never consented to VoR's surveillance activity, and therefore Mayer and the two other VoR employees may not claim immunity *ratione materiae*. (*p 24*)

R: VoR should have been immune from pre and post judgment measures of constraint. (*p. 23*)

VoR was established under a bilateral treaty for the purpose of strengthening "political, cultural, and artistic" life. As such it served governmental non-commercial functions. (p.*24*)

Neither country is a party to the U.N. Convention on Jurisdictional Immunities, nor does Article 15 reflect custom. (*p.24*)

Immunity *ratione materiae* is granted to every government agent for government acts. Therefore the VoR employees were entitled for immunity for their involvement in Carmen. (p.24)

4. Would the anticipated auctioning of VoR's property constitute unjust enrichment? (pp. 24-25)

A: Given variance in application unjust enrichment has not emerged as a general principle. (*p.24*)

Riesland's bad faith in spying should preclude it from raising an unjust enrichment claim in accordance with the jurisprudence of multiple arbitration case. (*p.25*)

R: Unjust enrichment is a general principle of international law (Iran-U.S Claims Trib.). (*pp. 24-25*)

Amestonia has no justification for the enrichment and there is no contractual or other remedy available for Riesland other than claiming compensation on the basis of unjust enrichment. (*p.25*)

QP3

1. Was Kafker's preventive detention legal under International Human Rights law? (pp. 26-30)

A: Kafker's detention was unreasonable, unnecessary, and disproportionate; thus, arbitrary.(*p.27*)

There is no evidence linking Kafker to the activities of the Hive outside of him visiting the website www.longlivethehive.com." (*p.27*)

Kafker's detention is unlawful as he has not been informed of the reasons of his arrest. (*p.28*)

Kafker has been detained for an unlawfully lengthy period of time, violating his right to speedy proceedings. (*p.28-29*)

The nature of the Internet and Riesland's exclusive control over the evidence allow for a lowered evidentiary standard in attribution in the cyber sphere (*p.37-38*)

Code similarities and the Report from AIT, coupled with statements by Riesland's Attorney General comprise inferences that the Court should liberally apply in attributing in the cyber-sphere. (*p.38*)

The code similarities and presence of "government computer networks" weigh strongly in favor of Riesland's responsibility for the attack. (*p.38-39*)

Riesland is further liable for not practicing due diligence in preventing an attack from within its own borders (*sic utere tuo ut alienum non laedas)*. (*p.40-41*)

R: Amestonia has presented no evidence linking Riesland with the attack, and any evidence presented is suspect due to the difficulty of attribution in the cyber sphere. (*p. 37-40*)

There is no compelling reason to lower the evidentiary standard for attribution as current international standards are more than sufficient. (*p. 37-38*)

Cyber attribution is precarious due to the many methods for hiding and cloaking activity on the Internet; therefore, the higher evidentiary standard of the Tallinn Manual must be adopted. (*p.39*)

Due Diligence obligations have not rise to the level of a customary obligation and are, at best, a non-binding best practice; further, the due diligence standard imposes unreasonable burdens on states as it is technologically impossible to fully secure networks. (*p.39*)

2. Was the cyber-attack an Internationally Wrongful Act? (pp. 41-45)

A: The cyber-attack arguably constituted a use of force as its effects caused great harm to Amestonian society and its judicial system. (p*p.40-41*)

The cyber-attack caused sufficient physical damage to Amestonian infrastructure to constitute a violation of territorial integrity and non-intervention. (*pp.42-43*)

The newspaper attack violated Amestonia's right to the freedom of expression by effectively closing its primary national newspaper (*Article 19 ICCPR)*. (*p.43*)

The law-firm attack violated Amestonian citizens' right to attorney-client privilege (*p.44*)

R: The cyber-attack is not a use of force as its effects did not rise to the severity or invasiveness of a use of force, nor was it of a military character. (*pp .40-41*)

The cyber-attack is not a violation of territorial integrity as data deletion does not rise to the level of "physical damage." (*pp.42-43*)

The ICCPR does not apply extraterritorially; further, the threat posed by the leaks to Riesland's national security justified the action under the doctrine of necessity. *(p. 44)*

The Compromis gives no evidence that the attacks caused any disruptions to the confidentiality of the information possessed by the law firm; (*p.44*)

Appendix E: Suggested Questions for the Oral Rounds

International Law Generally

1. Is there any priority or hierarchy of the sources of international law mentioned in Art. 38 of the ICJ Statute?
2. What is customary international law? What are the elements of customary international law?
3. When asserting a state's obligations under customary international law:
    a. Where can we find evidence of relevant State practice?
    b. What is *opinio juris*? How is it proven?
4. Is the ICJ bound by its prior decisions?
5. What specific remedies is the Applicant/Respondent seeking? Is the ICJ permitted by its Statute to grant those remedies?
6. What is the basis of standing for the party seeking relief?
7. What is the standard of proof with respect to this issue? Which party bears the burden of proof?
8. If this Court determines that the lack of factual certainty allows multiple, conflicting inferences, what should this Court do then?
9. If a state has conflicting obligations under two treaties (or a treaty on the one hand and customary international law on the other), which obligation controls? What principle does the Court use to determine which obligation controls?
10. What is the Court to do if it finds there is a lacuna in the law?

Question Presented 1

A. Admissibility of Leaked Documents As Evidence

1. Are you familiar with the doctrine of *crimen omnia ex se nata vitia* ("property obtained by crime is vitiated")? What role does it play in your analysis?
2. Has this Court ever rejected a request by a State to admit evidence? Has this Court ever addressed the question of admission of leaked documents as evidence?
3. What were the facts of the Corfu Channel Case? What weight should we give to the fact that despite recognizing that the minesweeping operation conducted by the UK violated Albanian sovereignty, the Court nonetheless accepted into evidence the information the UK gathered during the operation?
4. Does the fact that the documents the Court is asked to admit into evidence are all Rieslandic confidential materials, have any bearing on our analysis?
5. Are you familiar with the doctrine of "ex injuria jus non oritur" (law does not arise from injustice)? What is its significance in our case?
6. Are the documents Amestonia is asking to admit into evidence "reliable, authentic and of probative value"?
7. Should the Court be concerned with whether an admission of the documents into evidence could be perceived as legitimizing whistleblowing and the stealing of documents?

B. Legality of Riesland's Surveillance Programs

8. What is the status of the law of peacetime espionage? Has a court of law ever recognized certain acts of intelligence collection when done in peacetime to violate international law? Doesn't every State spy?

9. What is the *Lotus* Principle? Is it an absolute principle or subject to limitations?
10. Does the ICCPR apply extraterritorially? What is the jurisdictional basis on which the ICCPR is deemed applicable in the context of either the Verismo or Carmen programs? Has the ICCPR ever been applied in the context of surveillance programs?
11. What does an "arbitrary interference" with the right to privacy mean in the modern digital age? Were Riesland's surveillance programs served legitimate purposes? Were the programs strictly necessary as the term is defined in the jurisprudence of the ECtHR? Was there sufficient oversight over the programs to ensure the prevention of potential abuse?
12. Do public figures, such as former prime ministers or diplomats, still entitled to a right to privacy?
13. Are States allowed to spy on ambassadors and diplomatic missions? Under what circumstances? What does the international law on diplomatic immunities and privileges say?
14. Is Amestonia estopped from bringing any claims on the legality of Riesland's Surveillance activity given its tacit consent to the conduct in its intelligence sharing arrangement with Riesland?
15. Did the Verismo program, and in particular the placing of the recording pod on the undersea fiber optic cable, violate customary international law of the sea?
16. Isn't Riesland obligated to collect intelligence in counter terrorism, under both U.N. Security Council Chapter VII Resolutions and Treaty law? Does this fact relevant to our analysis?
17. Did Riesland violate Amestonia's territorial integrity or the principle of non-intervention by conducting either one of its surveillance programs?

Question Presented 2

1. Did the station cease to fulfill its functions, as the terms are defined under Article 36 of the Broadcasting Treaty? if so at what time?
2. How do we interpret ambiguous terms within a treaty? (see the words: "cessation", "functions")
3. It would seem that Article 14(4) and Article 36 of the Broadcasting Treaty contradict themselves? Does international treaty law have a method for resolving potential conflicts within a treaty's text?
4. What is the relationship between the Broadcasting Treaty and broader Diplomatic and Consular law, as reflected in the Vienna Convention on Diplomatic Relations, Vienna Convention on Consular Relations, and the Special Missions Convention?
5. What is the Clean Hands Doctrine? Has the ICJ ever employed it in deciding a case? Doesn't Riesland come to the Court with unclean hands?
6. What is the principle of "unjust enrichment"? Does it have any holding in international law? would allowing Amestonia to auction the VoR station and its equipment and make profit out of it constitute unjust enrichment?
7. Can a state obtain a forfeiture order against another state's property? What potential rules of international law are applicable with regards to civil and criminal forfeiture?
8. When can a state declare someone *persona non grata*? Is the doctrine of *persona non grata* relevant to our case given that there is no such provision within the Broadcasting Treaty? Isn't it the common practice of States to declare persona non grata when individuals enjoying immunities and privileges are found to have been involved in espionage?
9. Can Amestonia claim necessity as a circumstance precluding its wrongfulness?

10. Was the treaty still in force on 16 February 2015? Was the treaty properly terminated and if so under what grounds? Could the treaty been invalidated?
11. What weight should we give to the term "without prejudice to their privileges and immunities" as it appears in Article 23(1) of the Broadcasting Treaty?
12. How quickly can the removal of immunities and privileges under Article 36 come into action? Isn't there a grace period? Are there any procedural requirements of relevance?

Question Presented 3

1. What differentiates preventive detention and other types of detention? Are there any differences between preventative, administrative, and pre-trial detention?
2. What is the legal weight that should be given to the human rights committee's general comments/concluding observations/decisions on individual communications or state complaints?
3. Can a state derogate from the ICCPR and under what circumstances may it do so? In our present case, is there a time of public emergency which threatens the life of the nations, in Riesland? Did Riesland properly notified of its potential derogations?
4. What would constitute an arbitrary arrest/detention/deprivation of liberty under ICCPR Article 9?
5. Does the Terrorism Act as drafted, and as applied in the context of Kafker, violate Article 9 of the ICCPR?
6. Can the ICJ order a party to produce secret or confidential documents? Is the information that Riesland is requested to produce really secret, given the leaks posted on *The Ames Post* website?
7. Was Kafker duly notified on the reasons for his arrest? Was the fact that he was notified that he is being detained under the Terrorism Act sufficient to meet this standard? What has this Court ruled in the *Diallo* case in this regard?
8. From the jurisprudence of international and domestic courts, can we derive a temporal bar on preventative detention under the ICCPR Article 9(3) ("entitlement to trial within a reasonable time")? Is two years, too long of a period to detain someone without charge? Would four years be unreasonable? Would Five? Is the standard set by the Terrorism Act of 540 days maximum for detention a standard in international law?
9. What is the right to *Habeas Corpus*, and what role does it play in our case?
10. Is Kafker entitled to any compensation if found that he was arbitrarily detained?
11. The last terrorist threat discussed in the *Compromis* (the thwarted honey contamination plot) occurs on October 2014? What was Riesland's justification in re-issuing its terrorism alert on April and October 2015, respectively?
12. Is the National Security Tribunal an objective and independent Court? What weight should we give to the fact that the same judges that authorized the surveillance of Kafker (under the SSBA) were the ones who routinely extended his detention (under the Terrorism Act)? Is there any precedent of a surveillance oversight court being granted detention powers?
13. Is there State practice to establish the lawfulness of "closed materials" and "special advocates" procedures in counter-terrorism detentions and trials?

Question Presented 4

1. What are the rules on burden of proof in the ICJ's jurisdiction? Are the rules any different in the context of establishing attribution of a wrongful act to a State? Do the rules change further in the context of attributing cyber attacks to a State? Should the rules change?
2. Are you familiar with the doctrine of "*Sic Utere Tuo Ut Alienum Non Laedas*"? What is it? What role does it play in our case? Does this doctrine apply in cybersphere?
3. Can a state be responsible for a wrongful act by failing to meet its due diligence obligations? Are due diligence obligations primary or secondary obligations, and what is the difference between the two?
4. Has any State ever attributed a cyber attack to another State solely on the basis of IP tracing and code analysis? What are the limitations on attribution in cyber sphere and how do those effectuate the law (both *lex lata* and *lex feranda*)?
5. What is the Tallinn Manual? What legal weight does the Tallinn Manual hold in our case? Does international law apply to cyber activity?
6. Can state claim sovereignty over their cyber domain? Is there such a thing as e-borders or sovereignty over cyber infrastructures? If so what is its nature, and its limits?
7. Assuming that the cyber attack is attributable to Riesland, did it violate the right to freedom of expression/access to knowledge as defined under Article 19 to the ICCPR?
8. What were the facts of *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor Leste v. Australia)*? What was decided in the order for provisional measures? What relevance, if at all, does the Court's determination regarding "legal professional privileges" have in the context of the cyber attack on the law offices of Chester & Walsingham?
9. What is the "United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (which sits under the UN Office for Disarmament Affairs)? What legal weight should we give its reports?
10. Did the cyber attack constitute a use of force? If the attack was short of a use of force, did it constitute an unlawful intervention in the internal affairs of Amestonia? What other potential rules of international law might have been violated by this attack?
11. What were the facts of the Sony Hack (allegedly by North Korea)? What were the facts of the Pentagon hack (allegedly by Russia)? What were the facts of the U.S. Office of Personal Management (allegedly by China)? How could your legal analysis of the cyber attack against the *Ames Post* and Chester and Walsingham be applied in the context of these cyber attacks?

The 2016 Philip C. Jessup International Law Moot Court Competition

The State of Amestonia

v.

The Federal Republic of Riesland

The Case Concerning the Frost Files

BEST OVERALL MEMORIAL
(Applicant)

First Place – Applicant
Richard R. Baxter Award

Columbia University
United States (Team #176)