ON SUBMISSION TO THE INTERNATIONAL COURT OF JUSTICE

AT THE PEACE PALACE,

THE HAGUE, THE NETHERLANDS

ON 13 JANUARY 2016

CASE CONCERNING THE FROST FILES

STATE OF AMESTONIA

(APPLICANT)

V.

FEDERAL REPUBLIC OF RIESLAND

(RESPONDENT)

MEMORIAL FOR THE APPLICANT

TABLE OF CONTENTS

INDEX OF AUTHORITIES

STATE PLEADINGS	Page No.
Memorial of Fmr. Yugoslav Rep. of Maced. Vol.I, *Application of the Interim Accord of 13 September 2015 (Fmr. Yugoslav Rep. of Maced. v. Greece)* (2009), http://www.icj-cij.org/docket/files/142/16354.pdf	44
Memorial of Timor-Leste, *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austrl.)* (2014), http://www.icj-cij.org/docket/files/156/18698.pdf	42

STATEMENT OF JURISDICTION

The State of Amestonia ("Amestonia") and the Federal Republic of Riesland ("Riesland") hereby submit the present dispute to the International Court of Justice ("ICJ"), pursuant to Article 40(1) of the Court's Statute, in accordance with the Compromis for submission to the ICJ on the differences concerning the Frost files, signed in The Hague, The Netherlands, on the first day of September in the year two thousand fifteen. Both States accepted the jurisdiction of this Court pursuant to Article 36(1) of its Statute.

QUESTIONS PRESENTED

I. Whether *The Ames Post* files are admissible as evidence.

II. Whether the Verismo program violates the right to privacy, Riesland's EEZ obligations and customary law.

III. Whether the Carmen program violated diplomatic immunities and constituted an abuse of a right.

IV. Whether Amestonia upheld the Broadcasting Treaty or alternatively, legally terminated it due to a material breach.

V. Whether the arrest of VoR employees and seizure of its premises and property were in conformity with international law.

VI. Whether Amestonia enjoys the right to exercise diplomatic protection over Kafker.

VII. Whether Riesland's derogation from the ICCPR under the Terrorism Act was lawful.

VIII. Whether Kafker's arrest and subsequent proceedings violated the right to liberty and the right to fair trial under the ICCPR.

IX. Whether the cyber-attacks against *The Ames Post* and Chester & Walsingham law firm are attributable to Riesland and violated international law.

X. Whether the cyber-attacks are lawful countermeasures.

XI. Whether the burden of proof should shift to Riesland, or alternatively, be shared.

STATEMENT OF FACTS

BACKGROUND

Amestonia, a developing State, borders Riesland, which possesses a world-renowned IT and communications sector. Following decades of positive relations, in 1970 the States signed several cooperation agreements in areas such as trade, extradition and intelligence-sharing. Relations strengthened further in 1992 with the establishment of an agricultural free-trade area. Riesland eventually became the top importer for Amestonian produce.

That year, the States signed the Treaty on the Establishment of Broadcasting Facilities ("BT"), following which Riesland built and operated the Voice of Riesland television station ("VoR") in Amestonia. The appointed head of station, Margaret Mayer, hosted the popular program featuring interviews with leading Amestonians. The staff, premises and property received privileges and immunities subject to usage compatible with the station's functions and to the obligation to respect Amestonian law.

VIOLENT INCIDENTS IN AMESTONIA

Amestonian farmers rely on Riesland-produced neonicotinoid insecticides ("neonics") to boost yields. A 2012 Institute for Land and Sustainable Agriculture ("ILSA") report found correlations between neonics use and decreasing bee populations. Thereafter, public debate sparked within Amestonia and Riesland, aided by the 2013 launch of www.longlivethehive.com, a forum website which quickly gained attention in both States.

On 2 February 2014, seven Amestonian warehouses containing neonics were set on fire, resulting in the deaths of three Amestonian and two Rieslandic nationals, along with €75 million in damages and long-term negative health consequences. On 7 March 2014, Amestonian and

Rieslandic officials and individuals involved in farming and neonics production received envelopes, stamped with an image of a bee, containing non-toxic powder. Simultaneously, an anonymous tweet threatened further attacks.

Subsequently, Riesland offered its' security and intelligence services' cooperation in eliminating the threat, including the Rieslandic Secret Surveillance Bureau's ("RSSB"), which collects foreign intelligence pursuant to the Secret Surveillance Bureau Act 1967.

On 16 October 2014, RSSB director Tom Sivaneta informed Amestonia of environmental activists planning to contaminate a honey shipment intended for Riesland. The following day, seven months after the powder incident, Riesland declared a Terrorism Alert pursuant to the Rieslandic Terrorism Act ("RTA"), which has since been reissued twice, in April and October 2015.

On 21 October 2014, Amestonian police apprehended three students possessing chemically-altered neonics and maps of Amestonian honey-extraction facilities. They admitted to planning an attack and to being part of an organization called The Hive.

THE FROST REVELATIONS AND VERISMO

On 16 December 2014, former RSSB analyst Frederico Frost arrived in Amestonia seeking legal counsel from the Chester & Walsingham law firm ("C&W"). Perturbed by the creeping threat on liberty and sovereign equality the Bureau's secret operations pose, Frost gave C&W and *The Ames Post* newspaper a USB containing files downloaded from the Bureau's computers. Following independent authentication, in January and February 2015 the newspaper published selected documents detailing Rieslandic surveillance operations on Amestonia.

According to one document, published on January 23 and bearing Sivaneta's signature, the RSSB installed a recording pod on Amestonia's submarine primary backbone communications cable, located in Riesland's exclusive economic zone. The pod, which was part of the Verismo program authorized in May 2013, copied all cable data, transferring it to RSSB servers for analysis. Divers were later sent to the coordinates cited in the document and dismantled the device. Subsequent documents revealed that while the program was reviewed occasionally, its legality was never challenged.

On 2 February 2015, Riesland requested Frost's extradition and the recovery of the information. On 14 March, Amestonia refused the extradition on grounds of the "political offense" exception in the extradition treaty, following Riesland's failure to provide more details concerning the surveillance.

CARMEN AND SUBSEQUENT VOR EMPLOYEES' ARRESTS

Based on the Frost files, *The Ames Post* revealed the Carmen program on 16 February 2015. The program was initiated with Riesland's Foreign Minister's approval at the VoR's inception in order to advance Rieslandic political and economic interests. Under the program, RSSB agents doubled as VoR employees and physically hacked into Amestonian private sector leaders' and public figures' electronics during their interviews with Margaret Mayer. The agents then installed the "Blaster" malware which provided Riesland with full remote access to the devices. More than 100 of the most influential Amestonians were spied on, including Amestonia's Ambassador to the United Nations.

That evening, the VoR switched to reruns. Meanwhile, the Amestonian police obtained an emergency warrant to enter the premises and seize property, based on suspicion of criminal activity

aroused by the publication. The police found the station unattended and removed equipment and documents for use as evidence. The following morning, Margaret Mayer and two other VoR employees, attempting to flee by train to Riesland, refused to identify themselves at the Amestonian border and were subsequently arrested.

On 17 February 2015, Amestonia's President released a statement maintaining that Amestonia did not breach the BT, while condemning Rieslandic espionage as an excessive measure, even in the face of national security concerns. The Amestonian ambassador to Riesland was recalled for consultations, and the Amestonian TV station in Riesland officially closed. On 19 February, Riesland's Prime Minister defended the surveillance programs and accused Amestonia of a lack of reciprocity regarding counter-terrorism efforts.

KAFKER'S ARREST

Joseph Kafker is the retired founder of Amestonia's third largest party and is famously against the use of neonics in agriculture. On 7 March 2015, he was arrested after giving a speech at a conference in Riesland, based on undisclosed grounds, pursuant to the RTA. Amestonia was informed of Kafker's detention and denounced it, however Riesland denied all requests for evidence disclosure or his release.

Three days later, the National Security Tribunal first considered the case and ruled that all evidence was "closed material," making it unavailable for examination by Kafker. Based only on anonymous RSSB agents' testimonies, the Tribunal further extended his administrative detention, and continues its renewal every 21 days. Kafker was appointed a special advocate, who was nevertheless not permitted to consult with or offer him any information regarding allegations.

On 17 March 2015, *The Ames Post* published documents proving that the RSSB had gained access to Kafker's electronic devices through Carmen. The evidence collected through the operation consisted of linking Kafker to www.longlivethehive.com public chats. Nevertheless, Riesland's Attorney General stated that the State possessed evidence linking Kafker to senior Hive echelons.

Kafker has now entered his 385th day of detention without charge in a maximum-security prison, while a challenge to the proceedings' constitutionality was denied by the Rieslandic Supreme Court.

CYBER-ATTACKS AGAINST *THE AMES POST* AND CHESTER & WALSINGHAM

On 22 March 2015, cyber-attacks were launched against *The Ames Post's* and C&W's computer and communication switches. Consequently, master boot records were corrupted to the extent that 90% of the data was non-recoverable. This caused months-long delays to Amestonian court proceedings, an extended shutdown of *The Ames Post* and damages of €45-50 million.

The world-renowned Amestonian Institute of Technology, focused on computer science, determined the attacks originated from IP addresses associated with Rieslandic governmental computer infrastructure. Further, significant segments of code were exact replicas of the publically unavailable "Blaster" malware.

Riesland refused to clarify its involvement in the attacks, though Riesland's Attorney General claimed just days beforehand that Riesland will do whatever it takes to disrupt any further threats.

Following negotiations, the States turned to the ICJ in order to settle their differences peacefully.

SUMMARY OF PLEADINGS

I. The ICJ admits most evidence and weighs it according to circumstances. Further, even illegally obtained evidence may have significant bearing on the Court's decisions. Admitting the published *Ames Post* files thus conforms to the Court's procedure and practice, while the files' authenticity lends them weight.

Mass surveillance operations violate a customary prohibition and the right to privacy enshrined in the International Covenant on Civil and Political Rights ("ICCPR"), which applies extraterritorially, due to illegality and disproportionality. Additionally, States cannot interfere with others' submarine cables in their Economic Exclusive Zone. Operating Verismo thus violated international law, as it interfered with Amestonia's communications backbone in Riesland's EEZ.

Spying on diplomats violates their privacy and diplomatic immunities. Additionally, intentionally using rights for purposes different from their original scope constitutes an abuse. By operating Carmen, Riesland violated the ICCPR, diplomatic immunities and abused the Broadcasting Treaty ("BT") rights.

II. Treaties must be interpreted in good faith and reasonably reflect the parties' intentions in accordance with context, object and purpose of the treaty. A reasonable interpretation of the BT negates all immunities therein with the cessation of station functions. Hence, arresting VoR employees and confiscating property did not violate the BT.

Alternatively, treaties may terminate due to material breaches, including deliberate and persistent violations. Riesland's espionage violated its obligation to respect Amestonian law and to use VoR premises as envisaged in the treaty, constituting a material breach. In cases of special urgency,

treaties may terminate immediately upon notification. Considering the relevant circumstances, the BT terminated on 16 February 2015, with notification.

Immunity protecting State property from proceedings in foreign courts cannot be invoked when the property's purpose is commercial. Additionally, unjust enrichment cannot be claimed when States act illegally. Given the VoR's commercial broadcasting aim, it does not enjoy State immunity. Further, the espionage conducted within it was illegal, thus expropriation is not unjust enrichment.

In any event, necessity precludes wrongfulness. Amestonia fulfilled the relevant requirements regarding the VoR employees' arrests, thus precluding their wrongfulness.

III. States can exercise diplomatic protection over nationals who exhaust local remedies. Given that Kafker's claim was denied by Riesland's Supreme Court, Amestonia may exercise such protection.

A derogation from the ICCPR is lawful only when proportionate and when a threat exists to the nation's life. These conditions were not met, as The Hive attacks were not a severe threat and the derogation measures profiling non-nationals were disproportionate.

Assuming *arguendo* the derogation's legality, arbitrary detentions are impermissible, even during public emergencies. Riesland violated this by failing to provide Kafker with sufficient reasons for arrest and keeping him in an overly long pre-trial detention.

Additionally, States must guarantee a fair trial by allowing the accused to contest evidence and enjoy adequate legal counsel. Due to the closed and secret nature of the Tribunal, Kafker was denied this, thus his fair trial right was violated.

IV. State responsibility consists of attribution and wrongfulness. Attribution manifests, *inter alia*, through State organs' conduct or through the violation of due diligence obligations. The cyber-attacks against *The Ames Post* and Chester & Walsingham ("C&W") were linked to Riesland's Secret Surveillance Bureau, a State organ. Alternatively, Riesland failed to meet its due diligence obligation by neglecting to prevent the attacks from its territory, which is therefore attributable to it.

Riesland must respect territorial integrity as manifested in sovereignty over cyber infrastructure; respecting the non-intervention principle by refraining from coercively interfering with others' internal affairs; and respecting attorney-client privilege. By attacking Amestonian infrastructure, Riesland violated its territorial integrity and acted coercively in an effort to impact Amestonia's foreign policy, an internal affair. Additionally, Riesland's established access to confidential C&W communications with their clients violated the latter's attorney-client privilege. The attacks are thus internationally wrongful and Riesland is responsible for them.

Injured States must notify and offer negotiations before undertaking countermeasures, whose effects must be temporary and reversible. Riesland did not meet these requirements and the attacks are therefore not lawful countermeasures.

Finally, although the burden of proof generally lies upon the party alleging a fact, it may shift regarding authorities' misconduct towards private entities. As the attacks targeted private entities and originated from Riesland, the burden of proof should shift, or be shared.

PLEADINGS

I. THE PUBLISHED AMES POST FILES ARE ADMISSIBLE AS EVIDENCE; RIESLAND'S VERISMO AND CARMEN SURVEILLANCE PROGRAMS AGAINST AMESTONIANS REVEALED THEREIN VIOLATE INTERNATIONAL LAW, AND RIESLAND MUST CEASE THEM AND ASSURE NON-REPETITION

Amestonia contends that the published *Ames Post* files ("Frost files") are admissible [A]. Moreover, the Verismo [B] and Carmen [C] surveillance programs revealed therein violate international law, and Riesland must thus cease them and assure non-repetition [D].

A. THE AMES POST FILES ARE ADMISSIBLE

The published Frost files are admissible based on the Court's jurisprudence [1]. Notwithstanding, they are admissible even if obtained illegally [2].

1. The files are admissible

In determining evidentiary rules, the Court considers its objective to adjudicate substantively.[1] Generally, full admission of evidence is allowed,[2] except for procedurally improper submissions,[3]

---

[1] Statute of the International Court of Justice, 1 U.N.T.S. 993 (1945), art.30(1) [Statute]; Peter Tomka & Vincent-Joël Proulx, *The Evidentiary Practice of the World Court* 4 (N.U.S. Working Paper No.2015/010, 2015).

[2] Rules of Court, 1978 I.C.J. Acts & Docs. 6, art.62(1), 56(4); *Nuclear Tests (N.Z. v. Fr.),* [1974] I.C.J. 457, ¶15; CHESTER BROWN, A COMMON LAW OF INTERNATIONAL ADJUDICATION 90-92 (2009).

[3] Statute (n.1) art.52; *Free Zones of Upper Savoy and the District of Gex (Fr. v. Switz.)*, Order of Court, [1932] P.C.I.J. (Ser.A) No.22, 14, 21.

according to the case's circumstances.[4] In *Corfu*, significant weight was granted to circumstantial evidence gathered by one party when the evidence was under the other's exclusive control.[5] Some weight was also granted to news sources.[6] The State challenging evidence's admissibility must show grounds for exclusion.[7]

Amestonia contends that the files are admissible because they fulfil the procedural requirements, and in any case, the onus is on Riesland to prove otherwise.

2. The files are admissible even if obtained illegally

The Court has based decisions on evidence gathered illegally under international law,[8] since illegality only affects evidence's probative value following admission.[9] Similarly, a national security claim does not make leak-based evidence immaterial,[10] or inadmissible.[11] In determining this question, authenticity becomes relevant.[12]

---

[4] *South-West Africa (Eth. v. S.Afr; Liber. v. S.Afr.)*, Pleadings Vol.X, [1966] I.C.J. 3, 163.

[5] *Corfu Channel (U.K. v. Alb.)*, [1949] I.C.J. 4, 18 [*Corfu*].

[6] *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, [1986] I.C.J. 14, ¶63 [*Nicaragua*]; *U.S. Diplomatic and Consular Staff in Tehran (U.S. v. Iran),* [1980] I.C.J. 3, ¶12-13.

[7] DURWARD SANDIFER, EVIDENCE BEFORE INTERNATIONAL TRIBUNALS 179, 189-90 (1975).

[8] *Corfu* (n.5) 14.

[9] Tomka (n.1) 11.

[10] OPEN SOCIETY JUSTICE INITIATIVE, TSHWANE PRINCIPLES 39-40 (2013), https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

[11] *ConocoPhillips Petrozuata v. Venez.*, Decision on Respondent's Request for Reconsideration, I.C.S.I.D., ARB/07/30 (2014) (dissenting opinion of Georges Abi-Saab).

[12] SANDIFER (n.7) 202-06.

The Frost files are independently verified, and contain official letterhead and signature.[13] They were corroborated by coordinates allowing the pod's dismantling,[14] and police findings regarding Voice of Riesland ("VoR") equipment.[15] Assuming *arguendo* the files were obtained illicitly, this can only affect their weight, and does not exclude them altogether. Their authenticity is of importance in this determination. Therefore, the files are admissible and applicable.

B. In operating Verismo, Riesland violated its international obligations

By conducting mass surveillance, Riesland violated Amestonians' right to privacy [1], its exclusive economic zone ("EEZ") obligations [2] and a customary prohibition on mass surveillance [3].

1. By operating Verismo, Riesland violated Amestonians' right to privacy

Amestonia will establish that the International Covenant on Civil and Political Rights ("ICCPR") applies [a] and that Riesland violated it [b].

a. The ICCPR applies to Verismo

The ICCPR can apply extraterritorially through personal [i][16] or spatial [ii] models.[17]

---

[13] *Compromis*, ¶22, 25.

[14] Clarifications, ¶2.

[15] *Compromis*, ¶40.

[16] *Lopez-Burgos v. Uru.*, 52/1979, U.N.H.R. Comm., U.N. Doc.CCPR/C/13/D/52/1979 (1981), ¶12.2-12.3.

[17] *Armed Activities on the Territory of the Congo (D.R.C. v. Uganda)*, [2005] I.C.J. 168, ¶175-78; International Covenant on Civil and Political Rights art.2(1), 999 U.N.T.S. 171 (1966) [ICCPR];

i. The Personal Model

Human rights treaties apply to individuals under State authority and control, exercised by State agents.[18] Specifically, extraterritorial mass surveillance is a form of exercising control.[19]

Under Verismo, Riesland's Secret Service Bureau ("RSSB") agents tapped into the Amestonian communications backbone in order to conduct mass surveillance on Amestonians.[20] RSSB agents thus exerted control over these citizens' privacy and Riesland's ICCPR obligations apply.

ii. The Spatial Model

Alternatively, treaties apply when States have "effective overall control" over territory.[21] Jurisdiction applies when data is processed domestically, even when its subjects are located

---

MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES 127, 186-87 (2011).

[18] *Saldaño v. Arg.*, I.A.Comm.H.R., OEA/Ser.L/V/II.95 (1998), ¶17; *Issa v. Turk.*, E.Ct.H.R., 1821/96 (2004), ¶71; U.N.H.R. Comm., General Comment 31, U.N. Doc.CCPR/C/21/Rev.1/Add.13 (2004) [10]; *Al-Skeini v. U.K.*, E.Ct.H.R., 55721/07 (2011), ¶133-37 [*Al-Skeini*].

[19] U.N. High Commissioner H.R., *The Right to Privacy in the Digital Age*, ¶34, U.N. Doc.A/HRC/27/37, (2014) [UNHCHR]; Special Rapporteur, *Rep. on the Right to Privacy,* U.N. Doc.A/HRC/13/37 (2009) (by Martin Scheinin) [Scheinin]; Special Rapporteur, *Fourth Annual Rep.*, ¶41-43, U.N. Doc.A/69/397 (2014) (by Ben Emmerson) [Emmerson]; U.N.H.R. Comm., *Concluding Observations on the Fourth Periodic Rep. of the U.S.*, ¶21, U.N. Doc.CCPR/C/USA/CO/4 (2014).

[20] *Compromis*, ¶22, 29.

[21] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, [2004] I.C.J. 136, ¶109; *Loizidou v. Turk.*, E.Ct.H.R., 15318/89 (1996), ¶56; *Chiragov v. Arm.*, E.Ct.H.R., 13216/05 (2015), ¶57-69; Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81, 133-37 (2015) [Milanovic 2015]

elsewhere.[22] The ICCPR should be flexibly interpreted, as rigid interpretations defeat the convention's purpose in that they allow States to conduct foreign surveillance with impunity.[23]

Since communication data was stored and analysed on RSSB servers within Riesland,[24] the ICCPR applies.

b. Privacy was violated

The ICCPR prohibits "unlawful" or "arbitrary" privacy interferences,[25] which are examined based on interference [i];[26] legality [ii];[27] proportionality [iii];[28] necessity and legitimate aim.[29]

---

[22] *Liberty v. U.K.*, E.Ct.H.R., 58243/00 (2008), ¶66, 69-70 [*Liberty*]; ELECTRONIC FRONTIER FOUNDATION & ARTICLE 19, NECESSARY & PROPORTIONATE 3-9 (2014), https://en.necessaryandproportionate.org/files/2014/09/03/np-booklet-2014_english_final_print-ready-2-1_copy_0.pdf.

[23] Milanovic 2015 (n.21) 110-11.

[24] *Compromis*, ¶22.

[25] ICCPR (n.17) art.17.

[26] *Liberty* (n.22) ¶56-63; *Weber v. Ger.*, E.Ct.H.R., 54934/00 (2006), ¶73-138 [*Weber*]; Special Rapporteur, *Annual Rep. of the Office of the Special Rapporteur for Freedom of Expression*, 483, O.E.A. Doc./Ser.L/V/II.149 (2013) (by Catalina Botero).

[27] Emmerson (n.19) ¶29.

[28] Ibid., ¶51.

[29] Ibid., ¶35.

i. Privacy interference

Privacy includes confidentiality in private correspondence,[30] thus interception and storage of data and metadata from cyber correspondence constitute interferences.[31] Presence of legislation that allows secret surveillance, irrespective of use, is also a violation.[32]

Two interferences were made in the present case: SSBA legislation allowing electronic signals collection;[33] and interception, collection and storage of communication via Verismo.[34]

ii. Unlawful interference

Domestic legislation must uphold three criteria: accessibility, foreseeability and rule of law compatibility.[35] *Accessibility* denotes the legislation's public availability, and individuals' ability to challenge information;[36] *foreseeability* concerns clarity regarding conditions under which authorities may interfere with privacy;[37] *rule of law compatibility* encompasses safeguards including details of interference-worthy offences.[38]

---

[30] U.N.H.R. Comm., General Comment 16, U.N. Doc.HRI/GEN/1/Rev.1 (1994) [8] [GC16].

[31] *Kennedy v. U.K.*, E.Ct.H.R., 26839/05 (2010), ¶118; *Amann v. Switz.*, E.Ct.H.R., 27798/95 (2000), ¶69; *Escher v. Brazil*, [2009] I.A.Ct.H.R. (Ser.C) No.200, ¶114.

[32] *Klass v. Ger.*, E.Ct.H.R., 5029/71 (1978), ¶37 [*Klass*].

[33] *Compromis*, ¶4.

[34] Ibid., ¶22.

[35] *Liberty* (n.22) ¶15; UNHCHR (n.19) ¶23.

[36] *Zakharov v. Russ.*, E.Ct.H.R., 47143/06 (2015), ¶288, 300 [*Zakharov*]; *Haralambie v. Rom.*, E.Ct.H.R., 21737/03 (2009), ¶96.

[37] *Malone v. U.K.*, E.Ct.H.R., 8691/79 (1984), ¶67; *Kopp v. Switz.*, E.Ct.H.R., 23224/94 (2000), ¶72.

[38] *Weber* (n.26) ¶95; *Klass* (n.32) ¶49.

Although the SSBA is public, it is almost impossible to know about surveillance or correct information, since the collection is secret and untargeted.[39] Likewise, since the SSBA limits where the Bureau *cannot* collect extra-judicially rather than where it *can,*[40] foreseeability becomes virtually impossible. The SSBA criterion of "foreign intelligence" is similarly broad in that it uses "national security" as a blanket term to authorize surveillance.[41]

iii. Disproportionate interference

States must establish guarantees against abuse, including grounds for surveillance and prior independent review capable of granting "binding remedies".[42] Further, programs should target on a case-by-case basis,[43] for a particular aim.[44]

Existing safeguards to the SSBA are lacking: they allow *ex post facto* review, but no *ex ante* authorization; the reviewing bodies cannot grant binding remedies; and no notification is given once surveillance ceases.[45] Moreover, no criteria for target differentiation in Verismo exist, nor

---

[39] *Compromis*, ¶22.

[40] *Zakharov* (n.36) ¶248; *Compromis*, ¶5.

[41] *Compromis*, ¶4.

[42] *Digital Rights Ireland v. Minister for Communication* and *Kärtner Landesregierung,* E.C.J. C-293/12 and C-594/12 (2014), ¶62 [*Digital Rights*]; *Weber* (n.26) ¶106; Emmerson (n.19) ¶45-50, 61; *Zakharov* (n.36) ¶233, 249, 275.

[43] GC16 (n.30) [8].

[44] *Digital Rights* (n.42) ¶57, 69.

[45] *Compromis*, ¶5.

does case-by-case authorization.[46] Due to the above conditions, Riesland violated the ICCPR right to privacy.

2. Riesland violated its EEZ obligations

The EEZ is a customary regime granting all States the right to lay and maintain submarine cables, while coastal States only enjoy certain sovereign rights related to natural resources in their EEZ.[47] Accordingly, States must pay due regard to other States' cables inside their EEZ, over which their jurisdiction does not extend.[48]

Intercepting Amestonia's communications backbone in Riesland's EEZ[49] does not show due regard, which includes balancing relevant States' rights and a good faith obligation to negotiate differences.[50] Riesland's pod placement constitutes an interference and was done unilaterally, clandestinely, in bad faith and without due regard.

Further, data interception is not a permissible measure. The only interference allowed regarding cables in the EEZ is in order to explore or exploit natural resources, or in order to control pollution.[51] Riesland's actions serve neither, and are thus impermissible.

---

[46] Ibid., ¶22.

[47] United Nations Convention on the Law of the Sea art.56, 58(1), 1833 U.N.T.S. 3 (1982) [UNCLOS]; *Delimitation of the Maritime Boundary in the Gulf of Maine Area (Can./U.S.)*, [1984] I.C.J. 246, 294 [*Maine Gulf*]; R.R. CHURCHILL AND A.V. LOWE, THE LAW OF THE SEA 161-62 (3rd ed.,1999).

[48] Tara Davenport, *Submarine Communications Cables and Law of the Sea: Problems in Law and Practice* 43 OCEAN DEV. & INT'L L. 201, 211-14 (2012); UNCLOS (n.47) art.56, 58.

[49] *Compromis*, ¶22.

[50] *Fisheries Jurisdiction (U.K. v. Ice.)*, [1974] I.C.J. 3, 34.

[51] UNCLOS (n.47) art.79(2); Robert Beckman & Tara Davenport, *The EEZ Regime: Reflections After 30 Years, in* LOSI-KIOST CONFERENCE ON SECURING THE OCEAN FOR THE NEXT

3. Riesland violated the customary mass surveillance prohibition

By operating Verismo, Riesland violated a customary mass surveillance prohibition established by State practice [a] and *opinio juris* [b].[52]

a. State practice

State practice must be general, widespread, and consistent, especially among affected States, though not of particular duration.[53] It can be established by domestic legislation and judicial decisions,[54] as well as by UN General Assembly ("UNGA") resolutions.[55] A UNGA resolution critical of mass surveillance practices passed unanimously following the Snowden revelations.[56] Similarly, national rulings and laws check untargeted mass surveillance.[57] Thus, State practice

---

GENERATION 2, 21-24 (Harry Scheiber & Moon Sang Kwon, eds., 2012), https://www.law.berkeley.edu/files/Beckman-Davenport-final.pdf.

[52] Statute (n.1) art.38(1)(b); Special Rapporteur, *Second Rep. on Identification of Customary International Law,* 7-15, U.N. Doc.A/CN.4/672 (2014) (by Michael Wood) [Wood II].

[53] *North Sea Continental Shelf (Ger./Den.; Ger./Neth.),* [1969] I.C.J. 4, ¶73 [*North Sea*]; *Maine Gulf* (n.47) 299.

[54] *Jurisdictional Immunities of the State (Ger. v. It.: Greece intervening)*, [2012] I.C.J. 99, ¶55 [*Jurisdictional Immunities*]; Special Rapporteur, *Third Rep. on Identification of Customary International Law,* ¶58, U.N. Doc.A/CN.4/682 (2015) (by Michael Wood).

[55] OBED ASAMOAH, THE LEGAL SIGNIFICANCE OF THE DECLARATIONS OF THE GENERAL ASSEMBLY OF THE UNITED NATIONS 54 (1966).

[56] G.A. Res.68/167 (2014) [Res.68/167].

[57] USA FREEDOM Act of 2015, Pub. L. No.114-23, 129 Stat. 268 (2015); ACLU v. Clapper, 785 F.3d 787, 795 (2d Cir. 2015) (U.S.A.); X (Re), 2014 F.C.A. 249, ¶103 (Can.); Lei no.12.965 art.7, 10, de 23 Abril de 2014, D.O.U. de 24.4.2014 (Braz.); Davis v. Secretary of State for the Home Department, [2015] E.W.H.C. (Admin) 2092 (Eng.).

demonstrates a prohibition on mass surveillance that Riesland did not abide by in Verismo, given its unfettered collection of massive databases.[58]

b. Opinio juris

Opinio juris requires States' belief that they are applying customary international law,[59] and is evidenced by States' public statements,[60] protests,[61] and UNGA resolutions.[62] A mass surveillance prohibition can be understood from condemnations of practices revealed by Snowden,[63] alongside similar concerns voiced by several States regarding Riesland's surveillance.[64]

C. IN OPERATING CARMEN, RIESLAND VIOLATED PRIVACY AND DIPLOMATIC CORRESPONDENCE IMMUNITIES AND ABUSED A TREATY RIGHT

---

[58] *Compromis*, ¶22, 29.

[59] *North Sea* (n.53) 44; Wood II (n.52) ¶60.

[60] Louis Sohn, *Unratified Treaties as a Source of Customary International Law in* REALISM IN LAW-MAKING 231, 235 (Adriaan Bos & Hugo Siblesz eds., 1986).

[61] I.C. MacGibbon, *Customary International Law and Acquiescence* 33 BRIT. Y.B. INT'L L. 115, 124 (1957).

[62] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, [1996] I.C.J. 226, ¶70 [*Nuclear Weapons*].

[63] Res.68/167 (n.56); EUR. PARL. DOC.2013/2188(INI) (2014); Secretaría de Relaciones Exteriores de México, Comunicado 392 (2013), http://saladeprensa.sre.gob.mx/index.php/en/comunicados/3270-392; U.N. GAOR, 68th Sess., 5th plen. mtg., 7, U.N. Doc.A/68/PV.5 (2013).

[64] *Compromis*, ¶41.

By using the VoR station to spy on Amestonian public figures and diplomats, Riesland violated the right to privacy [1] and diplomatic correspondence immunities [2] while abusing a treaty-granted right [3].

1. Riesland violated the right to privacy

The ICCPR applies to Riesland's actions in Carmen [a] and its obligations under it were violated [b].

a. The ICCPR applies to Carmen

As stated above,[65] the ICCPR applies via the spatial model whereby "effective overall control" is demonstrated through governmental public powers usage with hosting States' permission.[66] The Treaty on the Establishment of Broadcasting Facilities ("BT") grants near-exclusive inviolability in the VoR, allowing Riesland executive control of the premises, as reflected in the obligation to protect against intrusions and disturbances.[67] In fact, Amestonian agents could enter the station only in exceptional circumstances.[68] Since Amestonia consented to this control, the ICCPR applies.

b. Privacy was violated

---

[65] *Supra* Pleading I(B)(1)(a)(ii).

[66] *Banković v. Belg.*, E.Ct.H.R., 52207/99 (2001), ¶71; *Al-Skeini* (n.18) ¶135; MILANOVIC (n.17) 137-41.

[67] *Compromis*, Annex I, art.14 [BT].

[68] Ibid.

As discussed above, interference [i] and legitimate aim [ii] are among the elements establishing a violation:[69]

i. Privacy interference

Collection of phone and internet correspondence constitutes an interference.[70] Accordingly, intelligence collected by hacking Amestonians' electronics constitutes an interference.[71]

ii. Illegitimate aims

National security and public safety are acceptable aims,[72] while advancing political and economic interests is not recognized in jurisprudence.[73] Carmen's aim of advancing Riesland's regional economic and political interests[74] is illegitimate. Riesland therefore violated the right to privacy.

2. Riesland violated diplomatic correspondence immunities

---

[69] *Supra* Pleading I(B)(1)(b).

[70] *Supra* (n.31).

[71] *Compromis*, ¶25.

[72] *Weber* (n.26) ¶103-04; *Van Hulst v. Neth.*, 903/1999, U.N.H.R. Comm., U.N. Doc.CCPR/C/82/D/903/1999 (2004), ¶3.8; Milanovic 2015 (n.21) 136.

[73] Ibid.

[74] *Compromis*, ¶26.

The Vienna Convention on Diplomatic Relations, to which both States are parties,[75] grants incumbent diplomats immunities, including a prohibition on surveillance and diplomatic correspondence inviolability.[76] Carmen interfered with Amestonian diplomats' correspondence[77] and thus violated these immunities.

3. Riesland abused a treaty right

The abuse of a right is an extension of the good faith principle.[78] According to it, a treaty-granted right must be exercised reasonably.[79] The intentional use of a right for a purpose different from its original scope, leading to injuries has been recognized as an abuse.[80] Relatedly, privacy intrusions constitute injuries.[81]

---

[75] Ibid., ¶43.

[76] Vienna Convention on Diplomatic Relations art.24, 27, 40(3), 500 U.N.T.S. 95 (1961); Jovan Kurbalija, *E-Diplomacy and Diplomatic Law in the Internet Era in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 393, 417-18 (Katharina Ziolkowski ed., 2013).

[77] *Compromis*, ¶26.

[78] Charter of the United Nations art.2(2) [UNC]; *Gabčíkovo-Nagymaros Project (Hung./Slovk.)*, [1997] I.C.J. 88, 95 (Separate opinion of Judge Weeramantry) [*Gabčíkovo-Nagymaros*]; *U.S.–Import Prohibition of Certain Shrimp and Shrimp Products*, W.T.O., WT/DS58/AB/R (1998), ¶156-58; BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 121 (Grotius 1987) (1953).

[79] Ibid., 125.

[80] Alexandre Kiss, *Abuse of Rights*, MPEPIL, Dec. 2006, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1371?rskey=pE3b3a&result=1&prd=EPIL.

[81] YILC, Vol.II (Pt.2), 92, art.31, cmt.5 (2001) [ARSIWA Commentary].

Riesland's right to establish the VoR extended only to the BT's purposes.[82] By using its premises for espionage that intruded on Amestonians' privacy, Riesland exceeded the treaty's scope of rights and caused injuries, thus abusing a right.

D. AMESTONIA IS ENTITLED TO CESSATION AND NON-REPETITION

States responsible for internationally wrongful acts are obligated to cease them and provide non-repetition assurances.[83] Accordingly, Riesland must cease its surveillance and espionage and assure non-repetition.

II. THE SEIZURE AND ARRESTS OF VOR PROPERTY AND EMPLOYEES DID NOT VIOLATE THE BROADCASTING TREATY OR OTHER INTERNATIONAL OBLIGATIONS

Amestonia contends that the arrests of Margaret Mayer and other employees and the expropriation of VoR property did not violate the BT [A] or other international obligations [B].

A. THE BT WAS NOT VIOLATED

Amestonia did not violate the BT because VoR employees' immunity and equipment inviolability were removed [1]. Alternatively, Amestonia legally terminated the treaty due to a material breach [2], pursuant to the procedural urgency exception [3].

---

[82] BT (n.67) pmble.

[83] Responsibility of States for Internationally Wrongful Acts, G.A. Res.56/83, Annex, art.30, U.N. Doc.A/RES/56/83 (2001) [ARSIWA].

1. Immunity and inviolability were removed

Given that the station's function is broadcasting [a], immunities and inviolabilities ceased pursuant to Article 36 of the BT [b].

a. The station's only function is broadcasting

Under the Vienna Convention on the Law of Treaties ("VCLT"), treaties must be interpreted in good faith, according to terms' ordinary meaning, object and purpose, and context.[84] Thus, treaties' terms must have reasonable meaning that respects parties' intentions in concluding the treaty,[85] without giving either side unfair advantages.[86] Context is derived from the title,[87] preamble,[88] and related provisions.[89]

Within the BT, the appropriate interpretation of "functions" is "broadcasting television programs": *first*, due to the text's ordinary meaning in context, the function is derived from the title and preamble ("*seeking* to offer… television channels"),[90] along with Article 2, which defines

---

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

[85] *Gabčíkovo-Nagymaros* (n.78) ¶142.

[86] MARK VILLIGER, COMMENTARY ON THE 1969 VIENNA CONVENTION ON THE LAW OF TREATIES 425-26 (2009).

[87] RICHARD GARDINER, TREATY INTERPRETATION 180 (2008).

[88] VCLT (n.84) art.31(2); *Whaling in the Antarctic (Austl. v. Japan: N.Z. Intervening)*, [2014] I.C.J. 226, ¶56.

[89] Ibid., 250; ANTHONY AUST, MODERN TREATY LAW AND PRACTICE 210 (3rd ed., 2013).

[90] BT (n.67) pmble.

the station's functions;[91] *second*, it does not give either party unfair advantages, such as unilateral unchecked data collection.

b. Immunities and inviolabilities ceased

The VoR's functions ceased when it was abandoned and switched to reruns.[92] If functions cease,[93] employees' immunities hold only if the relevant acts were "performed… in the exercise of its functions."[94] Thus, the treaty does not protect employees' espionage acts,[95] as these are not part of the station's function.

VoR property and premises also lose their inviolability due to cessation of functions.[96] Article 14(4) affords the station's archives inviolability "at all times." Given that Article 36 authorizes terminating all inviolabilities, the harmonious interpretation[97] of Article 14 would treat "at all times" as "at all times *of the treaty's operation*". Therefore, the inviolability is revocable through Article 36.

2. Alternatively, Amestonia legally terminated the treaty due to a material breach

---

[91] Ibid., art.2.

[92] *Compromis*, ¶27.

[93] BT (n.67) art.36.

[94] Ibid., art.15(1)(c).

[95] *Compromis*, ¶29.

[96] BT (n.67) art.36.

[97] Hersch Lauterpacht, *Restrictive Interpretation and the Principle of Effectiveness in the Interpretation of Treaties*, 26 BRIT. Y.B. INT'L L. 48, 81 (1949); AUST (n.89) 210.

Article 60 of the VCLT allows treaties' termination due to material breaches,[98] which are violations of provisions essential to treaties' object or purpose [a].[99] Breaches must be serious,[100] such as deliberate and persistent obligations violations [b].[101]

a. The BT's object and purpose

It is widely accepted that treaties' "object and purpose" are intertwined,[102] and that multiple objects and purposes can exist.[103] Several elements form the latter:[104] treaties' titles;[105] their aims, often derived from preambles;[106] and the text itself,[107] especially the first articles.[108]

---

[98] VCLT (n.84) art.60.

[99] Ibid., 60(3)(b).

[100] YILC, Vol.II, 255 (1966); THE VIENNA CONVENTION ON THE LAW OF TREATIES: A COMMENTARY VOL.II 1358 (Olivier Corten & Pierre Klein ed., 2011) [VCLT: COMMENTARY].

[101] *Legal Consequences for States of the Continued Presence of S.Afr. in Namib. (S.W.Afr.) notwithstanding Security Council Resolution 276 (1970)*, Advisory Opinion, [1971] I.C.J. 16, ¶95.

[102] VILLIGER (n.86) 427.

[103] Vesna Crnic-Grotic, *Object and Purpose of Treaties in the Vienna Convention on the Law of Treaties*, 7 ASIAN Y.B. INT'L L. 141, 172 (1997).

[104] Jan Klabbers, *Some Problems Regarding the Objects and Purpose of Treaties*, 8 FINNISH Y.B. INT'L L. 138, 155-56 (1997).

[105] *Certain Norwegian Loans (Fr. v. Nor.)*, [1957], I.C.J. 9, 24.

[106] *Sovereignty over Pulau Ligitan and Pulau Sipadan (Indon./Malay.),* [2002] I.C.J. 625, ¶49-51.

[107] *Nicaragua* (n.6) ¶273; IAN SINCLAIR, THE VIENNA CONVENTION ON THE LAW OF TREATIES, 130-35 (1984).

[108] VILLIGER (n.86) 428.

The BT preamble exhibits the treaty's object and purpose: "[fortifying] the friendship between the two countries".[109] Similarly, the title and first articles show these to be the regulation of broadcasting through establishing TV stations and producing programs.[110] Therefore, the BT's object and purpose is to strengthen friendship and operate TV stations.

b. The breach was serious, persistent and deliberate

Article 23(1) of the BT ensures respect for domestic law,[111] without which friendship and cooperation are impossible.[112] Article 23(2) forbids usage of the station incompatible with its functions.[113] Therefore, Article 23, which was breached, is essential to the object and purpose of the treaty.

Underground rooms made for spying; misleading backdoors; station employees doubling as Bureau engineers;[114] these prove that espionage, not broadcasting, was the VoR's main aim. Further, the RSSB, with the Foreign Affairs Minister's authorization, conducted these acts[115] from the station's inception,[116] in order "to advance Riesland's political and economic interests."[117] This

---

[109] BT (n.67) pmble.

[110] Ibid., art.1(1), 2.

[111] Ibid., art.23(1).

[112] RICHARD VINCENT, NONINTERVENTION AND INTERNATIONAL ORDER Ch. 9 (1974).

[113] BT (n.67) art.23(2).

[114] *Compromis*, ¶25.

[115] Ibid., ¶26; Clarifications, ¶5.

[116] *Compromis*, ¶25.

[117] Ibid., ¶25, 26.

implies that Riesland initiated the BT in order to conduct espionage. The acts constitute a material breach of Article 23 since their length, scope and severity satisfy the deliberate, persistent and serious requirements.

3. Further, Amestonia applied the procedural urgency exception

Article 65(1) of the VCLT instructs parties wishing to terminate treaties to first notify in writing[118] the other parties regarding the termination,[119] including its cause and reasoning.[120] Article 65(2) establishes a three-month moratorium between notification and actual termination. However, in cases of special urgency, such as sudden and serious treaty breaches,[121] this strict time limit may be compromised.[122] Furthermore, in *Gabčíkovo-Nagymaros*, Judge Herczegh stated that States anticipating breaches may act urgently to prevent them.[123]

On 17 February 2015, President Hale issued a written statement notifying termination.[124] He specifically addressed Rieslandic espionage as a BT violation and maintained that the search of the VoR and employee detentions were only undertaken following these revelations.[125] Amestonia

---

[118] VCLT (n.84) art.67.

[119] Ibid., art.65(1).

[120] VCLT: COMMENTARY (n.100) 1492.

[121] Ibid., 1496.

[122] YILC, Vol.II, 46 (1966); VILLIGER (n.86) 809.

[123] *Gabčíkovo-Nagymaros* (n.78) 198 (dissenting opinion of Judge Herczegh).

[124] *Compromis*, ¶29.

[125] Ibid, ¶30.

had to act urgently to ascertain the magnitude of the material breach, and to prevent Riesland from operating with impunity arising from the VoR employees' escape.[126]

B. AMESTONIA DID NOT VIOLATE ANY OTHER INTERNATIONAL OBLIGATION

Amestonia contends that it did not violate any other international obligation as Riesland's State immunity is inapplicable in this case [1]. Moreover, the planned auction of equipment is not unjust enrichment [2]. Alternatively, the arrests and seizures were based on necessity [3].

1. Riesland's State immunity is inapplicable

The VoR employees do not enjoy immunity from criminal jurisdiction for espionage [a], and the VoR property is not immune from enforcement as it was used for commercial purposes [b].

a. Criminal jurisdiction

Functional immunity ("*ratione materiae*") protects foreign State officials from criminal jurisdiction in relation to conduct performed in their official capacity.[127] However, officials do not

[126] Ibid, ¶28.

[127] *Prosecutor v. Blaškić*, Judgement on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997, I.C.T.Y., IT-95-14 (1997), ¶38 [*Blaškić*]; HAZEL FOX & PHILIPPA WEBB, THE LAW OF STATE IMMUNITY 515-516 (3rd ed., 2013).

enjoy immunity if the host State did not consent to their presence and activity in its territory,[128] especially regarding espionage.[129]

While Amestonia authorized the VoR employees' appointment, this was for the purpose of broadcasting,[130] and not espionage, as carried out by unauthorized Bureau engineers.[131] Hence, Margaret Mayer and the Bureau engineers are not immune from criminal jurisdiction.

b. Enforcement measures

State immunity protects States' property from proceedings before foreign courts.[132] Specifically, no post-judgment enforcement measures, including executive enforcement measures,[133] may be taken against States' property when used for non-commercial purposes.[134] The status of property is evaluated predominantly by its purpose,[135] which must be sovereign in

---

[128] Xiaodong Yang, *Jus Cogens and State Immunity*, 3 N.Z. Y.B. INT'L L. 131, 164-69 (2006); Special Rapporteur, *Second Rep. on Immunity of State Officials from Foreign Criminal Jurisdiction*, ¶53, U.N. Doc.A/CN.4/631 (2010) (by Roman Kolodkin).

[129] Ibid.; *Blaškić* (n.127) ¶41; *Certain Questions of Mutual Assistance in Criminal Matters (Djib. v. Fr.),* Oral Proceedings, [2008] I.C.J. 2, ¶24.

[130] *Compromis*, ¶7.

[131] Ibid., ¶25, 29.

[132] FOX (n.127) 89; United Nations Convention on Jurisdictional Immunities of States and their Property art.5, 18-19, adopted in G.A. Res.59/38 (2004) [UNCSI].

[133] Leo Bouchez, *The Nature and Scope of State Immunity from Jurisdiction and Execution,* 10 NETH. Y.B. INT'L L. 28-30 (1979); Dames v. Regan, 453 U.S. 654, 685 (1981) (U.S.A).

[134] *Jurisdictional Immunities* (n.54) ¶118; UNCSI (n.132) art.19(c).

[135] Ibid.; XIAODONG YANG, STATE IMMUNITY IN INTERNATIONAL LAW 392-94 (2012).

order to avoid this commercial exception. Regulation of services is considered commercial;[136] specifically, television broadcasting, even without advertising, is commercial.[137]

The BT's purpose is regulating broadcasting services,[138] and is thus commercial. Therefore, post-judgement measures taken against the VoR, in the form of an executive forfeiture order,[139] are outside the scope of State immunity.

2. The planned auction does not constitute an unjust enrichment

Unjust enrichment is a general principle of international law.[140] Nevertheless, the claiming State's wrongdoing is an exception to its invocation.[141] This practice is based on the principle *nemo auditur propriam turpitudinem suam allegans* ("no one will be heard relying on his own turpitude").[142] For example, in *Plama*, the violation of the hosting State's law was considered

---

[136] UNCSI (n.132) art.2(1)(c)(i); Reichler v. Liber., 484 F.Supp.2d 1, 2 (D.D.C. 2007) (U.S.A.).

[137] YANG (n.135) 78-79; Los Angeles v. Conus, 969 F.Supp. 579, 586 (C.D.Cal. 1997) (U.S.A.); Bryks v. Canadian, 906 F.Supp. 204, 207–208 (S.D.N.Y. 1995) (U.S.A.).

[138] *Supra* Pleading II(A)(2)(a).

[139] *Compromis*, ¶40.

[140] *Sea-Land Service v. Iran,* 6 Iran-U.S.C.T. 149, 168 (1986); *Saluka Investments B.V. v. Czech Partial Award* [2006] P.C.A. ¶449.

[141] Christina Binder & Christoph Schreuer, *Unjust Enrichment*, MPEPIL, Aug. 2013, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1002?rskey=BCyWSi&result=1&prd=EPIL.

[142] *Plama Consortium v. Bulg.*, I.C.S.I.D., ARB/03/24 (2008), ¶143.

deceitful conduct, precluding restitution;[143] and in *Inceysa*, the concealment of important facts before signing a contract constituted an undue conduct denying restitution.[144]

The VoR employees committed serious violations of Amestonian criminal law.[145] For decades, Riesland has engaged in a concerted, secret surveillance campaign targeting Amestonian citizens and important public figures.[146] Together, these facts constitute illegal and deceitful conduct, precluding an unjust enrichment claim.

3. Alternatively, the arrests and seizures were necessary

The customary Article 25 of the Articles on State Responsibility for Internationally Wrongful Acts ("ARSIWA")[147] provides four cumulative elements for necessity:[148] the act was meant to safeguard an essential interest [a]; the interest is threatened by grave and imminent peril [b]; it is the only means possible [c]; and the international community's essential interests will not be seriously impaired [d]. If the relevant obligation excludes the invocation of necessity,[149] or the State contributed to the situation's occurrence, [150] Article 25(2) precludes necessity. Neither exists here.

---

[143] Ibid.

[144] *Inceysa Vallisoletana SL v El Sal.,* I.C.S.I.D., ARB/03/26 (2006), ¶338.

[145] *Compromis*, ¶30.

[146] Ibid., ¶29.

[147] *Gabčíkovo-Nagymaros* (n.78) ¶51; *Sempra Energy International v. Arg.*, I.C.S.I.D., ARB/02/16 (2007), ¶344.

[148] ARSIWA (n.83) art.25(1); ARSIWA Commentary (n.81) 83-84.

[149] ARSIWA (n.83), art.25(2)(a).

[150] Ibid., art.25(2)(b).

a. The arrests were meant to safeguard an essential interest

Necessity may only be invoked to safeguard an essential interest,[151] determined on a case-by-case basis. In *CMS v. Argentina*, the need to avoid a major social, economic or political crisis was considered an essential interest.[152] The need to prevent a possible infringement of "the continued function of the State's essential services" also qualifies.[153]

Secrecy is essential to State functions such as foreign affairs and diplomacy.[154] The Carmen program gathered information about Amestonian policies in the advancement of Rieslandic interests.[155] Amestonian State functions' confidentiality was imperilled by Riesland, as evidenced by the Rieslandic Foreign Affairs Minister's knowledge of Amestonia's positions on upcoming U.N. votes and by espionage on Amestonian diplomats.[156]

b. A grave and imminent peril

---

[151] ARSIWA (n.83), art.25(2)(a).

[152] *CMS Gas Transmission v. Arg.*, I.C.S.I.D., ARB/01/8 (2005), ¶319.

[153] YILC, Vol. II (Pt.1), 14 (1980) [Ago Report].

[154] YILC, Vol.II, 102 (1958).

[155] *Compromis*, ¶26.

[156] Ibid.; Clarifications, ¶5.

The interest must be imperilled by a present danger whose occurrence is beyond the threatened State's control,[157] as established by evidence reasonably available at the time.[158] This Court defined peril as an act invoking the idea of risk rather than actual, material damage.[159]

Information gathered through Carmen was used maliciously, as the phone of Amestonia's Ambassador to the UN was hacked and used for information extraction.[160] If Mayer and the other employees had succeeded in crossing into Riesland,[161] it would hardly have been possible to know what information they possessed, thus maintaining the risk of future grave occurrences beyond Amestonia's control.

c. The arrests were the only means possible

Necessity is excluded if other means are available, even more expensive or less convenient ones.[162] Methods that could aggravate the situation should be avoided.[163]

Considering that the VoR employees were apprehended at the border whilst fleeing Amestonia by train,[164] and that relevant information was available only within VoR premises, no other means existed to ascertain the exact scope of espionage in order to prevent further harm.

---

[157] Ago Report (n.153) 19-20.

[158] JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 184 (2003) [Crawford Commentary].

[159] *Gabčíkovo-Nagymaros* (n.78) ¶54.

[160] Ibid., ¶26.

[161] *Compromis*, ¶28.

[162] Crawford Commentary (n.158) 184; *Gabčíkovo-Nagymaros* (n.78) ¶56-57.

[163] Ibid., 198 (dissenting opinion of Judge Herczegh).

[164] *Compromis*, ¶28.

d. The arrests and seizures did not seriously impair an essential Rieslandic interest

Breached interests must be of lesser importance than safeguarded ones.[165] The functioning of State services is essential to sovereignty,[166] which is a fundamental principle of international law.[167]

While Amestonia respects the freedom of Riesland's nationals and property, these are not essential interests and cannot outweigh the interests of a whole nation and the continuation of its State functions.[168] Therefore, the arrests and seizures did not seriously impair an essential Rieslandic interest, and necessity is met.

III. KAFKER'S DETENTION VIOLATED INTERNATIONAL LAW, ENTITLING AMESTONIA TO HIS IMMEDIATE RELEASE, COMPENSATION AND THE DISCLOSURE OF ALL INFORMATION FORMING THE BASIS FOR HIS APPREHENSION

Amestonia contends that Kafker enjoyed diplomatic protection [A]. Additionally, the declaration of a Terrorism Alert leading to his apprehension derogated unlawfully from the ICCPR [B], or, alternatively, violated Articles 9 [C] and 14 [D] of the ICCPR.

---

[165] Roman Boed, State of Necessity as a Justification for Internationally Wrongful Conduct, 3 YALE H.R. & DEV. L.J. 1, 18 (2000); *Gabčíkovo-Nagymaros* (n.78) ¶58; Crawford Commentary (n.158) 83-84; Sarah Heathcote, *Circumstances Precluding Wrongfulness in the ILC Articles on State Responsibility: Necessity in* THE LAW OF INTERNATIONAL RESPONSIBILITY 498 (James Crawford, Alain Pellet & Simon Olleson eds., 2010).

[166] Ago Report (n.153) 14.

[167] UNC (n.78) art.2(4).

[168] *Supra* Pleading II(B)(3)(a).

A. AMESTONIA EXERCISES DIPLOMATIC PROTECTION OVER KAFKER

States may invoke customary diplomatic protection of nationals who exhausted local remedies[169] in pursuing the "essence of the claim" as far as local law permits,[170] save for exceptional circumstances,[171] including consecutive decisions adverse to the individual.[172] Kafker's detention has been extended every 21 days for 7 months without factual change,[173] making the reviews adversely repetitive. Additionally, Riesland's Supreme Court ruled on the matter.[174] Hence, Kafker, an Amestonian national, has exhausted local remedies, and is entitled to diplomatic protection.

B. RIESLAND'S TERRORISM ALERT DEROGATED UNLAWFULLY FROM THE ICCPR

Derogating from ICCPR obligations during emergency requires a nation's life to be threatened, and the derogation to be necessary, proportionate and indiscriminate.[175] Riesland failed to meet these requirements, as no threat existed [1], and the derogations were disproportionate [2].

---

[169] *Ahmadou Sadio Diallo* (*Guinea v. D.R.C*), Preliminary Objections, [2007] I.C.J. 582, ¶39 [*Diallo* Preliminary]; YILC, Vol.II (Pt.2) 24, 2(2) (2006).

[170] *Elettronica Sicula S.p.A (ELSI)* (*U.S. v. It.*), [1989], I.C.J. 15, ¶59-60 [*ELSI*]; CHITTHARANJAN AMERASINGHE, DIPLOMATIC PROTECTION 141 (2008).

[171] *Diallo* Preliminary (n.169) ¶44.

[172] *ELSI* (n.170) ¶60-61.

[173] *Compromis*, ¶33.

[174] Ibid.

[175] ICCPR (n.17) art.4(1).

1. No public emergency existed

Public emergencies are exceptional crises threatening organized life within States.[176] Threats must be actual, present, imminent, and so severe that routine criminal enforcement measures are insufficient for handling them.[177] Emergency declarations must be frequently reviewed, and withdrawn when possible.[178]

State practice concerning terrorism-based emergency declarations is scarce.[179] The vast majority of derogations followed severe attacks that resulted in numerous fatalities and significant damage to property.[180] Accordingly, the recent French derogation followed terrorist attacks that killed 128 people and injured many more.[181]

Riesland suffered the deaths of two nationals in the warehouse fire, and no damage occurred within its territory.[182] While tragic, this event's severity does not amount to a public emergency. Moreover, the first declaration was issued 7 months after the powder incident, following the

---

[176] *Lawless v. Ire.*, E.Ct.H.R., 332/57 (1961), ¶28.

[177] *Den., Nor., Swed. and Neth. v. Greece*, E.Ct.H.R., 3321/67, 3322/67, 3323/67 and 3344/67 (1969), ¶113; U.N.H.R. Comm., *The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR*, ¶54, UN. Doc.E/CN.4/1985/4 (1984) [*Siracusa*].

[178] U.N.H.R. Comm., *Concluding Observations on the U.K. and N.Ire.*, ¶23, U.N. Doc.CCPR/C/79/Add.55 (1995).

[179] Martin Scheinin & Mathias Vermeulen, *Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines that Seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight Against Terrorism* 23 (E.U.I. Working Paper No.2010/08, 2010).

[180] Ibid.

[181] Council of Europe, Declaration from the Permanent Representation of France, dated 24 November 2015, http://www.bioeticayderecho.ub.edu/en/node/3196.

[182] *Compromis*, ¶14.

discovery of the honey pollution threat.[183] This later matter was less serious, and could have been adequately dealt with by security authorities, who had already communicated the relevant information to their Amestonian counterparts.[184]

Furthermore, even if the situation during the first declaration was severe enough, Riesland has not been threatened since the honey pollution scare in October 2014.[185] Considering the lack of evidence regarding threats posed by The Hive, Riesland had no basis for subsequent declarations.[186]

2. The derogation measures are disproportionate

Derogations may limit rights only if required by the situation.[187] This proportionality requirement is reflected in the duration and severity of derogations.[188] Specifically, unjustified discrimination based on nationality is considered disproportionate.[189] The European Court of Human Rights ("ECtHR"), which is greatly respected by this Court,[190] found in *A. v. UK* that nationality-based counter-terrorist emergency legislation was disproportionate, as the threat was

---

[183] Ibid., ¶18.

[184] Ibid.

[185] Ibid., ¶19.

[186] Ibid., ¶18; Clarifications, ¶7.

[187] ICCPR (n.17) art.4(1); U.N.H.R. Comm., General Comment 29, U.N. Doc.CCPR/C/21/Rev.1/Add.11 (2001) [4].

[188] Ibid; *Siracusa* (n.177) ¶51.

[189] Special Rapporteur, *Implementation of G.A. Resolution 60/251,* ¶32, U.N. Doc.A/HRC/4/26 (2007) (by Martin Scheinin).

[190] *Ahmadou Sadio Diallo (Guinea v. D.R.C.)*, [2010] I.C.J. 639, ¶68 [*Diallo*].

also home-grown,[191] as is often the case with terrorism.[192] Further, while the right to liberty is derogable, proportionality is hinged on the existence of some safeguards,[193] such as the option to view the evidence basing the allegations and proper legal representation.[194]

A plausible option exists that some Hive members are Rieslandic given the facts: www.longlivethehive.com's popularity in both States;[195] three Amestonian deaths; and the damage solely to Amestonian property resulting from the arson.[196] Thus, the Rieslandic Terrorism Act's ("RTA") nationality-based detention is discriminatory.[197] Moreover, there were no safeguards for Kafker's liberty: the National Security Tribunal ("the Tribunal") deemed all evidence "closed material," completely unavailable to the detainee[198] and only available to advocates within the proceedings, though communicating it to the detainee was prohibited.[199] Therefore, Riesland unlawfully derogated from the ICCPR.

C. ALTERNATIVELY, KAFKER'S ARREST VIOLATED ICCPR ARTICLE 9

---

[191] *A. v. U.K.*, E.Ct.H.R., 3455/05 (2009), ¶186 [*A./U.K.*].

[192] HELEN DUFFY, THE WAR ON TERROR AND THE FRAMEWORK OF INTERNATIONAL LAW 388 (2nd ed., 2015).

[193] OREN GROSS & FIONNUALA NÍ AOLÁIN, LAW IN TIMES OF CRISIS 250 (2006).

[194] *Askoy v. Turk.*, E.Ct.H.R., 21987/93 (1996), ¶81; *Brannigan v. U.K.*, E.Ct.H.R., 14554/89 (1993), ¶49-50.

[195] *Compromis*, ¶13.

[196] Ibid., ¶14.

[197] *Compromis*, Annex II, art.3(a) [RTA].

[198] Ibid., art.3(e).

[199] Ibid., art.3(i).

Article 9(1) of the ICCPR prohibits arbitrary detentions.[200] This rule is fundamental and may not be derogated from even during public emergencies.[201] To avoid arbitrariness, detention procedures must conform to the other requirements and safeguards detailed in Article 9,[202] including providing reasons for the arrest and respecting the right to trial within a reasonable time.[203]

Riesland arbitrarily arrested Kafker, as it did not provide sufficient reasons for the arrest [1], and Kafker's pre-trial detention violates his right to a trial within a reasonable time [2].

1. Sufficient reasons for arrest were not provided

Article 9(2) stipulates that every person shall promptly receive reasons for their arrest.[204] These must include the general legal basis for the arrest and enough factual specifics, such as the wrongful act itself, to indicate the allegation's substance.[205] National security as the sole given basis for arrest is insufficient.[206] Further, even in cases of national security, the information must be provided immediately upon arrest.[207]

---

[200] ICCPR (n.17) art.9(1).

[201] U.N.H.R. Comm., General Comment 35, U.N. Doc.CCPR/C/GC/35 (2014) [66] [GC35].

[202] Ibid; U.N. High Commissioner H.R., *Fact Sheet No.26*, sec.IV(B) (2000).

[203] GC35 (n.201) ¶4.

[204] ICCPR (n.17) art.9(2).

[205] GC35 (n.201) ¶25; *A./U.K.* (n.191) ¶218.

[206] *Caldas v. Uru.*, 43/1979, U.N.H.R. Comm., U.N. Doc.CCPR/C/OP/2 (1990), ¶13.2; DUFFY (n.192) 713-14.

[207] GC35 (n.201) ¶27; *Ismailov v. Uzb.*, 1769/2008, U.N.H.R. Comm., U.N. Doc.CCPR/C/101/D/1769/2008 (2011), ¶7.2.

Riesland only informed Kafker that he was detained in accordance with the RTA;[208] no additional information was given. This general notification does not specify facts connecting him to The Hive or to any of the attacks, and thus denies him the ability to effectively answer the allegations, thus violating Article 9(2).

2. Violation of the right to trial within a reasonable time

Article 9(3) provides that detainees should be tried within a reasonable time or released.[209] Considering that pre-trial detention presents severe risks of prolonged, arbitrary detention,[210] it should only be applied when necessary and when no alternatives exist.[211] Possible alternatives, not amounting to deprivation of liberty,[212] include pre-trial control orders as adopted by the UK, enforcing house arrests and electronic tagging.[213] The criteria to evaluate whether pre-trial detention is excessively long includes the complexity of the case and the accused's behavior.[214] The complexity criterion is the relevant one here, and is measured by the time needed to collect and process information. In *Teesdale v. Trinidad and Tobago*, a 16-month pre-trial detention was

---

[208] *Compromis*, ¶32.

[209] ICCPR (n.17) art.9(3).

[210] U.N.H.R. Comm., *Concluding Observations on Colombia*, ¶20, U.N. Doc.CCPR/C/COL/CO/6, (2010); N.S. Rodley, *Detention as a Response to Terrorism*, *in* COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE 457, 473 (Ana Salinas de Frias et. al., eds., 2012).

[211] GC35 (n.201) ¶15.

[212] *A./U.K.* (n.191) ¶20.

[213] Independent Reviewer on the Prevention of Terrorism Act 2005, *Final Report,* 4-8 (2012) (by David Anderson).

[214] GC35 (n.201) ¶37; LOUISE DOSWALD-BECK, HUMAN RIGHTS IN TIMES OF CONFLICT AND TERRORISM, 293 (2011).

considered excessive given that all the evidence for prosecution was gathered and no additional investigations were held.[215]

Kafker has now entered his 385th day of pre-trial detention which may still be extended to a total of 540 days;[216] only then would criminal proceedings begin. Kafker is a respected dignitary and does not pose a direct threat;[217] hence his maximum-security detention is unnecessary, and alternatives, such as supervised house arrest, should have been considered. Riesland claims to possess evidence directly linking Kafker to The Hive's senior echelons and terrorism acts[218] and has not asserted that it needs further investigation in this matter. Therefore, Riesland should either press charges against Kafker or release him.

D. ALTERNATIVELY, KAFKER'S TRIAL BEFORE THE TRIBUNAL VIOLATED ICCPR ARTICLE 14

Article 14 of the ICCPR provides various fair trial guarantees,[219] and is applicable to acts that are criminal in nature, regardless of their qualification in domestic law.[220] Article 14(1) enshrines the fundamental principle of equality of arms: that the same procedural rights should be provided to all parties.[221] Emergency derogations from this principle are justified only if they do not entail

---

[215] *Teesdale v. Trin. & Tobago*, 677/96, U.N.H.R. Comm., U.N. Doc.CCPR/C/74/D/677/1996 (2002), ¶9.3.

[216] RTA (n.197) art.3(h); *Compromis*, ¶32.

[217] *Compromis*, ¶32, 36.

[218] Ibid.

[219] ICCPR (n.17) art.14.

[220] *Osiyuk v. Belr.*, 1311/04, U.N.H.R. Comm., U.N. Doc.CCPR/C/96/D/1311/2004 (2009), ¶7.3; U.N.H.R. Comm., General Comment 32, U.N. Doc.CCPR/C/GC/32 (2007) [15] [GC32].

[221] Ibid., ¶13; ICCPR (n.17) art.14(1).

actual disadvantages to the defendant.[222] Equality of arms was not maintained since Kafker was prohibited from contesting all evidence adduced by the other party [1],[223] and did not enjoy adequate legal counsel [2].[224]

1. Kafker could not contest the evidence

The right to challenge evidence leading to arrest manifests in granting the accused access to all evidence used against him,[225] as well as in allowing him to examine witnesses.[226]

The use of anonymous testimony is permissible if there is justification for maintaining the witnesses' anonymity,[227] mostly related to the danger inflicted upon them.[228] However, the nature of the witness's duty is relevant: in *Van Mechelen*, the ECtHR found that public testimony would not expose policemen to threats, as it was part of their duty.[229] Even when anonymity is allowed,

---

[222] GC32 (n.220) ¶13; *Dudko v. Austrl.*, 1347/05, U.N.H.R. Comm., U.N. Doc.CCPR/C/90/D/1347/2005 (2007), ¶7.4.

[223] *Jansen-Gielen v. Neth.,* 846/1999, U.N.H.R. Comm., U.N. Doc.CCPR/C/71/D/846/1999 (2001), ¶8.2.

[224] GC32 (n.220) ¶32.

[225] ICCPR (n.17) art.14(3)(b); GC32 (n.220) ¶32-33.

[226] Ibid; ICCPR (n.17) art.14(3)(e).

[227] DOSWALD-BECK (n.214) 350.

[228] *Doorson v. Neth.,* E.Ct.H.R., 20524/92 (1996), ¶72-76.

[229] *Van Mechelen v. Neth.,* E.Ct.H.R., 21427/93 and 21363/93 (1997), ¶59-63.

the accused must be given the factual basis that led to the allegations,[230] and the judgment cannot be based solely on secret evidence or anonymous testimony.[231]

The Tribunal allowed RSSB officers to anonymously testify, despite their security-related position and without any known threat to them.[232] Additionally, it ruled all evidence pertaining to Kafker's activities "closed material,"[233] thus making no factual basis available to him.[234] Finally, the extension of Kafker's detention was based solely on anonymous testimonies and other secret evidence, which remain undisclosed to Kafker. In sum, Kafker was denied ICCPR fair trial guarantees.

2. Additionally, Kafker did not enjoy adequate legal counsel

Article 14(3)(b) provides the right to communicate with counsel of one's choosing.[235] Legal counsels should be able to advise and represent without restrictions or undue interference.[236] The use of special advocates in times of emergency is authorized only when advocates are provided with the evidence leading to arrest; when detainees are provided with sufficient information about the allegations against them; and when they are allowed to give the special advocate effective

---

[230] *Jasper v. U.K.,* E.Ct.H.R., 27052/95 (2000), ¶51.

[231] *Luca v. It.,* E.Ct.H.R., 33354/96 (2001), ¶40.

[232] *Compromis*, ¶33.

[233] Ibid.

[234] RTA (n.197) art.3(e).

[235] ICCPR (n.17) art.14(3)(b).

[236] GC32 (n.220) ¶34.

instructions.[237] Nevertheless, the practice is highly criticized even within States who use it and by special advocates themselves.[238]

Riesland selected a special advocate to represent Kafker during detention.[239] However, he was unable to inspect the closed material outside of proceedings,[240] and was prohibited from consulting with his client or sharing any information substantiating the allegations against him.[241] Thus, Kafker did not enjoy adequate legal counsel, which amounts to unfair trial.

IV. THE CYBER-ATTACKS AGAINST AMESTONIAN INSTITUTIONS ARE INTERNATIONALLY WRONGFUL AND ATTRIBUTABLE TO RIESLAND, ENTITLING AMESTONIA TO COMPENSATION

Amestonia contends that the cyber-attacks against *The Ames Post* and Chester and Walsingham ("C&W") are attributable to Riesland [A]; they violated Amestonia's territorial integrity, the non-intervention principle and attorney-client privilege [B]; and are not lawful countermeasures [C]. Finally, the burden of proof should shift to Riesland, or, alternatively, be shared [D].

A. THE ATTACKS ARE ATTRIBUTABLE

1. State organs conducted the attacks

---

[237] *A./U.K.* (n.191) ¶220.

[238] U.K. Joint Comm. H.R., *Counter-Terrorism Policy and Human Rights* 49-55 (HL Paper 157 HC 394) (2007).

[239] *Compromis*, ¶33.

[240] RTA (n.197) art 3(e).

[241] *Compromis*, ¶33.

Responsibility arises when conduct is wrongful and attributable.[242] Under ARSIWA, States are responsible for their organs' conduct,[243] with organs' status determined by function or internal law.[244] As intelligence service functions are governmental,[245] their conduct is attributable to States.[246]

Amestonia's world-renowned Institute of Technology traced the attacks to Rieslandic governmental infrastructure, while significant code segments, unknown in public usage, match the RSSB's "Blaster" malware.[247] The RSSB is a legally established intelligence service;[248] hence, the attacks are attributable to Riesland.

2. Alternatively, due diligence was not met

---

[242] ARSIWA (n.83) art.2.

[243] Ibid., art.4(1).

[244] Ibid., art.4(2); *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro),* [2007] I.C.J. 43, ¶392.

[245] Simon Chesterman, *We Can't Spy... If We Can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing Inherently Governmental Functions,* 19 EJIL 1055, 1070 (2008).

[246] Scheinin (n.19) ¶21; Group of Governmental Experts, *Rep. on Developments in the Field of Information and Telecommunications in the Context of International Security,* ¶13(c)(h), U.N. Doc.A/70/174 (2015) [GGE].

[247] *Compromis.*, ¶38; Clarifications, ¶8.

[248] *Compromis*, ¶3-4.

Due diligence obligates States to prevent wrongful acts in their territory to their best ability, and mitigate damages and prevent recurrence.[249] Due diligence applies to cyberspace,[250] and constitutes both a primary obligation,[251] and a path for attribution.[252] The obligation's content depends on the degree of harm predictability,[253] territorial control,[254] and is sensitive to States' capabilities,[255] especially technological development.[256] Cyber-attacks originating from governmental infrastructure indicate State involvement.[257]

These cyber-attacks originated from governmental infrastructure, indicating Rieslandic association and a high degree of control.[258] Being technologically developed,[259] Riesland's

---

[249] *Alabama Claims (U.S. v. U.K.),* 29 U.N.R.I.A.A. 125, 129-31 (1871); *North Sea* (n.53) 83.

[250] Michael Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68, 73 (2015) [*Defense*]; THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 5 (Michael Schmitt ed., 2013) [TALLINN].

[251] Vassilis Tzevelekos, *Reconstructing the Effective Control Criterion in Extraterritorial Human Rights Breaches,* 36 MICH. J. INT'L L. 129, 154 (2014).

[252] *Corfu* (n.5) 23; Jan Hessbruegge, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. INT'L L. & POL. 265, 299 (2003-2004); *Defense* (n.250) 78-79.

[253] *Chapman (U.S. v. Mex.)*, 4 U.N.R.I.A.A. 632 (1930); I.L.A., STUDY GROUP ON DUE DILIGENCE IN INTERNATIONAL LAW 3 (2014) [ILA].

[254] *Boyd (U.S. v. Mex)*, 4 U.N.R.I.A.A. 380 (1928); *Pulp Mills on the River Uruguay (Arg. v. Uru.)*, [2010] I.C.J. 14, ¶197 [*Mills*].

[255] ILA (n.253) 27*; Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion, [2011] I.T.L.O.S., ¶117.

[256] ARSIWA Commentary (n.81) 148, art.3, cmt.12-13.

[257] TALLINN (n.250) rule 7.

[258] *Compromis*, ¶38.

[259] Ibid., ¶1.

infrastructure is prone to harmful activities,[260] establishing high predictability of harm.[261] Riesland is capable of detecting harmful interferences, especially within governmental infrastructure, and should have prevented the attacks even if conducted by private actors. It also failed to mitigate damages, like prosecuting those responsible. In sum, Riesland failed to meet its due diligence obligation, and is responsible for the cyber-attacks.

B. THE CYBER-ATTACKS VIOLATED INTERNATIONAL LAW

Riesland violated Amestonia's territorial integrity, [1] the non-intervention principle [2] and attorney-client privilege [3].

1. Territorial integrity was violated

Enshrined in the UN Charter,[262] territorial integrity obligates States to respect boundaries and territorial inviolability.[263] As States possess sovereignty over territorial cyber infrastructure,[264] operations affecting another State's infrastructure may violate sovereignty, especially when causing physical damage.[265]

---

[260] Oona Hathaway, *The Law of Cyber-Attack* 100 CAL. L. REV. 817, 842 (2012).

[261] *Defense* (n.250) 74.

[262] UNC (n.78) art.2(4).

[263] *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.),* [2015] I.C.J. 1, ¶4 (declaration of Vice-President Yusuf); UNCLOS (n.47) art.301.

[264] GGE (n.246) ¶27; Patrick Franzese, *Sovereignty in Cyberspace: Can it Exist?* 64 AIR FORCE L. REV. 1, 33 (2009); *Defense* (n.250) 72; TALLINN (n.250) rule 1.

[265] Ibid., cmt.6.

Cyber infrastructure within Amestonian territory suffered physical damage: communication switches were disabled and master boot records corrupted, resulting in long delays in Amestonian court proceedings, an extended shutdown of *The Ames Post* and €45-50 million in damages.[266] Accordingly, Amestonian territorial integrity was violated.

2. The non-intervention principle was violated

The customary non-intervention principle recognizes States' political independence.[267] Prohibited interventions affect internal affairs – matters over which States may decide freely,[268] such as the formulation of foreign policy[269] – and employ coercion.[270] Coerciveness depends on the act's aim,[271] hence a threat of force may constitute coercion.[272]

---

[266] *Compromis*, ¶38.

[267] UNC (n.78) art.2(1)(7); *Corfu* (n.5) 35.

[268] *S.S. "Lotus" (Fr. v. Turk.),* [1927] P.C.I.J. (Ser.A) No.3, 18; G.A. Res.25/2625 (1970); G.A. Res.20/2131, ¶1 (1965); *Nicaragua* (n.6) ¶205.

[269] Ibid., ¶205.

[270] ANDREW CLAPHAM, BRIERLY'S LAW OF NATIONS 450 (2012).

[271] Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 429 (2011).

[272] UNC (n.78) art.2(4); Marco Roscini, *Cyber Operations as a Use of Force, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 233, 250 (Nicholas Tsagourias & Russell Buchan eds., 2015); Hathaway (n.260) 843.

A threat is comprised of States' implicit or explicit demonstration of intent to use force.[273] A cyber-attack constitutes a threat when the threatened act, if carried out, would be unlawful.[274] Amestonia contends that Riesland's cyber-attacks constitute a threat.

By showcasing damaging capabilities, Riesland demonstrated a willingness to compel Amestonia to succumb to Riesland's demand to extradite Frost,[275] a matter over which it is entitled to decide freely. The attacks therefore compromised Amestonia's right to independently formulate and apply its foreign policy.[276] The attacks meet the criteria of a prohibited intervention and are wrongful.

3. Riesland violated attorney-client privilege

Pursuant to the ICCPR, individuals are entitled to fair trial,[277] including confidential communication with counsel.[278] Attorney-client privilege, also considered a general principle of law,[279] is essential for the fulfilment of a fair trial.[280] Amestonia contends that attorney-client

---

[273] IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 364 (1963).

[274] *Nuclear Weapons* (n.62) ¶47; TALLINN (n.250) rule 12.

[275] *Compromis*, ¶24.

[276] AURELIU CRISTESCU, THE RIGHT TO SELF-DETERMINATION 27 (1981).

[277] ICCPR (n.17) art.14(1).

[278] Ibid., art.14(3)(b); GC32 (n.220) ¶34.

[279] *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austl.)* Request for the Indication of Provisional Measures [2014] I.C.J. 147, ¶24, 27 [*Timor-Leste*]; *Libananco Holdings v. Turk.*, I.C.S.I.D., ARB/06/8 (2008), ¶78, 80 [*Libananco*].

[280] Michael Karnavas, *Attorney-Client Privilege Part III: International Tribunals*, MICHAELKARNAVAS.NET/BLOG, Oct. 2015, http://michaelgkarnavas.net/blog/2015/10/07/privilege-part-iii/.

privilege applies to Riesland's actions through the ICCPR [a] or, alternatively, as a general principle of law [b], and that Riesland violated it [c].

a. The ICCPR applies through the personal model

Riesland accessed C&W files. The presence of the "Blaster" segments, which grants users full privileged access,[281] indicates that the RSSB had access to confidential correspondence in C&W computers.[282] By establishing access, Rieslandic State agents exercised authority and control over clients' privilege and by extension, their fair trial. Therefore, the ICCPR applies through the personal model, specifications abovementioned.[283]

b. Alternatively, attorney-client privilege applies as a general principle

All States recognize the principle of confidential communications between legal advisers and their clients.[284] As general principles apply to all legal fields,[285] attorney-client privilege applies to Riesland's actions as well.

c. Riesland violated attorney-client privilege

---

[281] *Compromis*, ¶25, 38.

[282] Ibid., ¶20.

[283] *Supra* Pleading I(B)(1)(a)(i).

[284] D.L.A. PIPER, LEGAL PRIVILEGE HANDBOOK (2013); LINKLATERS, PRIVILEGED (2013); Memorial of Timor-Leste, *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Austrl.)* ¶6.2, 6.6 (2014), http://www.icj-cij.org/docket/files/156/18698.pdf; *AM&S Europe v. Commission of the European Communities*, E.C.J., C-155/79 (1982), ¶18; *Libananco* (n.279) ¶78-80; *Timor-Leste* (n.279) ¶24-27.

[285] MARK JANIS, AN INTRODUCTION TO INTERNATIONAL LAW 46 (4th ed., 2003).

As demonstrated, communications between clients and attorneys are confidential,[286] pursuant to the ICCPR and as a general principle, founded upon fundamental fair trial rights, primarily the right for counsel.[287] It is non-derogable except under specific, limited circumstances based on client consent or criminality.[288] Establishing access to such communications, even without obtaining information, is a violation, as it jeopardizes clients' ability to trust that communications will remain confidential, and communicate openly with counsel.[289] In *Timor-Leste*, Judge Cançado Trinidade stated that confidential documents, although sealed, should be removed from Australia's hands and delivered to Court custody.[290]

Assuming *arguendo* that Riesland did not learn the communications' content, their confidentiality was nonetheless jeopardized. Riesland therefore violated attorney-client privilege.

C. THE ATTACKS ARE NOT LAWFUL COUNTERMEASURES

Pursuant to ARSIWA, countermeasures are allowed in response to prior wrongfulness, to induce States to satisfy their obligations.[291] Countermeasures' lawfulness depends upon certain

---

[286] GC32 (n.220); I.C.C. Rules of Procedure and Evidence, rule 73, U.N. Doc.PCNICC/2000/1/Add.1 (2000) [ICC Rules].

[287] Karnavas (n.280).

[288] ICC Rules (n.285) rule 73(a); The Special Tribunal for Leb. Rules of Procedure and Evidence, rule 163(ii), STL-BD-2009-01-Rev.6-Corr.1 (2009); *Situation in the C.A.R.*, Decision on the Prosecutor's Request, I.C.C., ICC-01/05-52-Red2, (2014), ¶4.

[289] *Prosecutor v. Popović,* I.C.T.Y, IT-05-88-A (2012), ¶7; Lauren Frank, *Ethical Responsibilities and the International Lawyer: Mind the Gap*, 2000 ILL. L. REV. 957, 972 (2000); American Bar Association, *Comment on Rule 1.6 in* MODEL RULES OF PROFESSIONAL CONDUCT ¶2, 18 (2013).

[290] *Timor-Leste* (n.279) ¶42, 53, 63 (dissenting opinion of Judge Cançado Trinidade).

[291] ARSIWA (n.83) art.49(1); *Portuguese Colonies* (*Naulilaa*) U.N.R.I.A.A. 1011, 1025–26 (1928); ELENA PROUKAKI, THE PROBLEM OF ENFORCEMENT IN INTERNATIONAL LAW 221 (2010).

conditions,[292] such as, *inter alia*, temporariness and reversibility,[293] and prior notification,[294] except in the case of urgent countermeasures.[295]

Riesland failed to communicate its intentions [1] and the attacks were irreversible in character [2] thus, the cyber-attacks were not lawful countermeasures.

1. Riesland's notification failure

Two preconditions exist for undertaking countermeasures:[296] *first*, responsible States must be called upon to fulfil their obligations;[297] *second,* injured States must notify their intention to undertake countermeasures, and offer negotiations.[298] Though States may adopt urgent countermeasures when necessary to preserve their rights, these conditions must nevertheless be undertaken *ex post facto*.[299] Analogues to VCLT Article 65, notifications must proclaim a decision to employ countermeasures, and indicate measures to be taken.[300]

---

[292] ARSIWA (n.83) art.52.

[293] *Gabčíkovo-Nagymaros* (n.78) ¶87.

[294] Michael Schmitt, *Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 717 (2014) [*Threshold*].

[295] David Bederman, *Counterintuiting Countermeasures*, 96 AM. J. INT'L L. 817, 825 (2002).

[296] ARSIWA (n.83) art.52(1).

[297] TALLINN (n.250) rule 9, cmt.4.

[298] *Threshold* (n.294) 717.

[299] ARSIWA (n.83) art.52(2).

[300] ARSIWA Commentary (n.81) 119; VCLT (n.84) art.65(1); Memorial of Fmr. Yugoslav Rep. of Maced. Vol.I, *Application of the Interim Accord of 13 September 2015 (Fmr. Yugoslav Rep. of Maced. v. Greece)* ¶5.44 (2009), http://www.icj-cij.org/docket/files/142/16354.pdf.

Following the documents' publication,[301] Riesland requested information recovery,[302] but failed to notify or offer negotiations. Notification cannot be inferred from Deloponte's statement, which lacked reference to a specific decision and details of the perpetrated measures.[303] With the documents published, no right or interest remained to preserve. Even assuming that Riesland was entitled to urgent countermeasures, it afterwards failed to notify or offer negotiations.

2. Alternatively, the attacks' permanent character

Countermeasures' effects must be reversible,[304] as a reflection of their purpose of returning to lawful relations.[305]

The cyber-attacks resulted in 90% of *Ames Post* and C&W data being non-recoverable,[306] and thus permanently affected. Therefore, the attacks were not lawful countermeasures.

D. RIESLAND BEARS THE BURDEN OF PROOF

[301] *Compromis*, ¶23.

[302] Ibid., ¶24.

[303] Ibid., ¶35.

[304] ARSIWA (n.83) art.49(3); *Gabčíkovo-Nagymaros* (n.78) ¶87.

[305] *Threshold* (n.294) 714.

[306] *Compromis*, ¶37.

Generally, the party alleging a fact must prove it.[307] However, this principle is not absolute.[308] Amestonia contends that the burden should shift [1] or, alternatively, be shared [2].

1. The burden of proof should shift

The burden of proof depends on the circumstances and facts necessary to establish.[309] One State's distinct advantage in access to information may constitute grounds for burden reversal.[310] As fact verification in cyberspace requires advanced technological capabilities,[311] technologically developed States are advantaged.[312] In *Diallo*, this Court held that regarding authorities' misconduct towards individuals, the burden may shift to the authority, best able to demonstrate compliance.[313]

---

[307] *Sovereignty over Pedra Branca/Pulau Batu Puteh, Middle Rocks and South Ledge (Malay./Sing.),* [2008] I.C.J. 12, ¶45.

[308] *Mills* (n.254) ¶162; *Maritime Delimitation in the Black Sea (Rom.* v. *Ukr.),* [2009] I.C.J. 61, ¶68*; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croat. v. Serb.)*, [2015] I.C.J. 43, ¶172-74.

[309] *Diallo* (n.190) ¶54.

[310] Michael Scharf & Margaux Day, *The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences*, 13 CHI. J. INT'L L. 123, 127-28 (2012).

[311] Scott Shackelford & Richard Andres, *State Responsibility for Cyber Attacks* 42 GEO. J. INT'L L. 971, 982 (2011).

[312] Ibid., 984.

[313] *Diallo* (n.190) ¶55-56.

Since the attacks originated from Rieslandic governmental infrastructure,[314] their documentation is especially accessible to Riesland. Being more technologically advanced than Amestonia,[315] Riesland is best placed to provide evidence and should therefore bear the burden.

2. Alternatively, the parties should share the burden

In any case, Reisland should cooperate in providing evidence.[316] In *Diallo*, States shared the burden regarding governmental misconduct towards private entities.[317] Furthermore, in *Corfu*, the Court held that States in whose territory wrongful acts occurred may need to provide explanations.[318]

As the attacks originated from Rieslandic infrastructure and territory, harming private entities,[319] Amestonia should not solely bear the burden.

---

[314] Clarifications, ¶9; *Compromis*, ¶37.

[315] Ibid., ¶1-2.

[316] *Mills* (n.254) ¶163.

[317] *Diallo* Preliminary (n.169) ¶56.

[318] *Corfu* (n.5) 18; Scharf (n.310) 130-31.

[319] Ibid., ¶37

PRAYERS FOR RELIEF

Amestonia respectfully requests this Honorable Court to adjudge and declare that:

1. The published Frost files are admissible as evidence and the surveillance programs revealed therein violate international law, obligating their cessation and non-repetition.
2. The seizure of VoR property and equipment, and the arrest of VoR employees, did not violate the Broadcasting Treaty or any other international obligations.
3. Kafker's detention violates international law, entailing his immediate release, disclosure of all information related to his apprehension, and compensation.
4. The cyber-attacks are attributable to Riesland and constitute internationally wrongful acts requiring compensation.