MUNLAWS 2023

FACULTY OF LAW, UNIVERSITY OF LJUBLJANA

FICTIONAL CASE

OSCE COURT OF CONCILIATION AND ARBITRATION

CHAIRS: LEA ZAHRASTNIK, ROK TRETJAK

This project
is sponsored by
the North Atlantic
Treaty Organisation

Pravna fakulteta
Univerza v Ljubljani

MUNLAW**S** 2023

FACULTY OF LAW, UNIVERSITY OF LJUBLJANA

FICTIONAL CASE

OSCE COURT OF CONCILIATION AND ARBITRATION

MUNLawS 2023

OSCE Court of Conciliation and Arbitration

THE CASE CONCERNING CYBER SECURITY AND ARTIFICIAL INTELLIGENCE

THE KINGDOM OF AVRELIA v. REPUBLIC OF RAPTORIA

Table of Contents

1 The Republic of Raptoria

1. The Republic of Raptoria (hereinafter: Raptoria) has a population of 130 million people. The State's capital and largest city is Raptorus. Raptoria is a sovereign country, with its own sovereign government. Raptoria is a developing country and home to a multi-ethnic population. It is a member of the United Nations, the Council of Europe, the OSCE, the GUAM organization and is a founding member of the Confederacy of Independent States (hereinafter: CIS), whose aim is to promote economic cooperation between its members. Raptoria has in place its Cyber Legal Act of 2002 (hereinafter: Cyber Legal Act), which has been developed on the line of the UNCITRAL Model Law on Electronic Commerce of the United Nations which was adopted by the General Assembly of the United Nations in the end of January 1997. The Cyber Legal Act provides the basis for the growth of electronic commerce and the digital ecosystem in the country. As a result, the digital economy of Raptoria has been growing at a remarkable pace.

2. Raptoria has a large number of natural rivers, which have a very strong water current. Consequently, Raptoria has various hydroelectricity plants that have been installed in various parts of the country. As of now, there are 15 major hydropower plants installed amongst the two longest rivers in the country which generate huge volumes of electricity that goes into the Central Electrical Grid of Raptoria. The Central Electrical Grid of Raptoria also supplies power to various other neighboring countries, including the Kingdom of Avrelia.

3. The Central Electrical Grid of Raptoria complies with a variety of security measures and procedures and has implemented standard parameters for protecting and preserving the cyber security of the data resident therein. Moreover, it also follows the following cyber security norms:

- Backups of critical software installers;
- Properly tuned firewalls between network segments;
- A password reset policy for VPN’s and administrative accounts;
- Backup and recovery tools for taking digital images from systems in the supervisory environment and data historian systems every 6 months.

2 The Kingdom of Avrelia

4. On the south, Raptoria is bordered by the Kingdom of Avrelia (hereinafter: Avrelia), which is home to approximately 170 million people. Avrelia attaches great importance to participation in international economic organizations and plays an active role in international security and technology development. Avrelia is also a member of the CIS.

5. The CIS was founded based on the efforts of Raptoria in the year 2004. Its main aims are to improve the overall economic prosperity and cooperation within the region, via promoting free trade and the free movement of workers. The founding document of the CIS is the Treaty on the Functioning of the Confederacy of Independent States (hereinafter: Treaty). Over the years, 15 States have signed the Treaty, including Raptoria in 2004 and Avrelia in 2005. To further engage in bilateral exchange, a declaration of cooperation between Avrelia and Raptoria was ratified by both States' respective parliaments on the 11th of February 2014 (see: Appendix II). Despite these mutual cooperation efforts, maintaining good relations between both States was sometimes perceived as challenging - as for example in 2017.

6. In 2017, a massive series of floods hit Avrelia's westernmost neighboring country, The Nation of Ered Luin, which caused a massive wave of immigration into Avrelia. Fearing that this wave of refugees would make their way to Raptoria, the Raptorian government preemptively reinstated border checks on its border with Avrelia, which were suspended since 2013. This decision was accompanied by a press release stating the following:

"The Republic of Raptoria recognises the importance of maintaining a welcoming and inclusive society. However, recent events have raised concerns about the influx of immigrants from the neighboring Nation of Ered Luin. These concerns primarily pertain to national security, public safety, and the ability to provide adequate resources and support for incoming individuals.

Raptorian officials have been closely monitoring the situation, and this decision to reintroduce border checks, is not taken lightly. It is a measured response intended to strike a balance between humanitarian principles and the need to safeguard the interests of Raptoria and its people."

7. This decision was met with outrage and disapproval by the Avrelian government which issued its own press release:

"The Kingdom of Avrelia regrets and disapproves of the recent announcement by the Republic of Raptoria to reinstate border checks along their shared border. This decision, driven by unfounded fears and a lack of understanding, not only impedes the free movement of people and goods but also constitutes a clear violation of the Treaty on the Functioning of the Confederacy of Independent States.

Avrelia has always valued the principles of the Confederacy, which include the free movement of people and goods among member nations. These principles were established to promote cooperation, economic growth, and peaceful coexistence among our nations. By reintroducing border checks, Raptoria undermines the very essence of this agreement."

3 Cybersecurity breach

8. On the 26th of June 2020, a major cyber security breach took place in the Central Electrical Grid of Raptoria, and as a consequence completely diverted the electricity supply to various destinations. An enormous amount of electricity was hijacked from there and sent to undisclosed locations. Furthermore, a vast amount of electricity was sent to some recipients in Raptoria. Due to these increased units that were supplied to them, critical information installations (such as Government facilities, the Stock-Exchange, the Public health sector, the Energy sector, Banking and Finance etc.) got damaged.

9. In addition, huge proportions of electricity got transmitted to Avrelia, even though there was no specific request or prior consent for it. This resulted in damaged and weakened systems and networks in Avrelia. That further affected economic activities, stock-exchange market and trading, which caused the economies of Raptoria and Avrelia daily losses of more than half a billion Euros.

10. Later on it was revealed that the breach affected various transmission and distribution system operators who were attacked in the long-term. The cyber attackers supposedly used different technical tools such as spear phishing to gain access to their business networks, theft of credentials from those business networks, use of virtual private networks (VPNs), use of remote access tools etc.

11. Meanwhile, the new government of Raptoria suspended the Cyber Legal Act and instead notified the international public of a new Cyber Security Law (see: Appendix I). This law was passed with the view to protect the sovereign interests and cyber security of Raptoria. The law came up with sweeping powers given to the government.

12. The most important provisions of the new Cyber Security Law are:

- The establishment of the new government agency, namely The National Agency for Cyber Security (NACS), which is responsible for cyber security on the national level;
- The NACS has the following powers and authorities:
    - Extrajudicial powers to investigate and prosecute any case related to cyber terrorism, even if it is out of its jurisdiction;
    - The authority to monitor all outgoing and ingoing internet traffic coming into Raptoria;
    - The power and ability to shut down the entire sector of Raptoria's internet systems to prevent the spread of cyber terrorism.
- The Government has stronger evidence-gathering powers - these include an extended legal duty upon individuals to preserve evidence, and a new "seize and

shift" power (the power to seize evidence and search through it at a later date) when conducting inspections;
- Everyone who attempts to obstruct, delay, or provide false information during investigations or who refuses to comply with solutions to cyber security problems will be subject to harsher civil sanctions;
- The Cyber Security Law also imposed a complete ban on VPNs by private individuals.

13. On the 1st of July 2020, the NACS detected another unauthorized entry into the Central Electrical Grid. The NACS responded quickly and shut down the entire internet sector in which the main control system was located. The Agency also used its new powers to track the source of the attack, which was revealed to be a remote and long-discontinued outpost in Avrelia which previously belonged to the now-defunct National Espionage Agency of Avrelia (NEAA).

14. On the morning of the 2nd of July 2020, the Prime minister of Raptoria summoned the Avrelian ambassador to explain why these attacks were coming from inside government facilities in Avrelia. The ambassador explained that although the NEAA was officially dissolved in 2010, it has continued to operate as a rogue shadow organization that the government of Avrelia has unsuccessfully attempted to stop for the last decade.

15. On the 18th of July, the NACS detected another attack, this time aimed at the national defense headquarters of Raptoria. The attack was yet again tracked back to the remote outpost in Avrelia. Due to the possible fallout, if the attackers were able to take control over the entire defense infrastructure of Raptoria (which includes a large arsenal of intercontinental ballistic missiles), the NACS took the unprecedented step of temporarily (until there is no clear course of action from Avrelia to stop the attack and any further attacks) disabling the entire internet for Avrelia, which stopped the attack.

16. The sudden and unexpected loss of internet for the entire State caused massive economic damage, as well as a major loss of life for Avrelia. On the 19th of July 2020, Avrelia expelled all Raptorian diplomats and demanded an immediate response from the government of Raptoria, which responded and said that the move was necessary to protect their interests and only came as a result of Avrelia's repeated failure to combat cyber terrorism.

4 Damage assessment

17. On the 20th of July 2020, the Senior Analyst of the Avrelian National Security Department (ANSD) issued a damage assessment report (see: Appendix III) ordered by the Avrelian government. The purpose of the assessment was to evaluate the extent of damage caused

by the decision of the Raptorian government to disable all internet connections in Avrelia, as well as to scrutinize the basis for this decision.

18. The assessment report stated that the decision by the Raptorian government to disable all internet connections in Avrelia had far-reaching and devastating consequences. Furthermore, it stated that the internet shutdown inflicted disproportionate harm on the population of Avrelia, and alternative strategies for addressing cyber threats should be explored with a focus on international cooperation and diplomacy.

19. In response to the damage assessment report, the Raptorian Ministry of Foreign Affairs issued a statement (see: Appendix IV), which read that while they respect the Analyst's expertise, they fundamentally disagree with several key points and conclusions put forth in the report. They stated that their decision to disable the internet in Avrelia was driven by a compelling need to protect their national security interests. Furthermore, they emphasized that they remain committed to safeguarding their nation from cyber threats and are open to diplomatic solutions to resolve the ongoing crisis.

5 The Court of Conciliation and Arbitration

20. The Court of Conciliation and Arbitration, based in Geneva, provides a mechanism for the peaceful settlement of disputes between States. The Court was established by the Convention on Conciliation and Arbitration within the OSCE (hereinafter: the CCA Convention), to which both Raptoria and Avrelia have acceded. The mechanism can be activated unilaterally by any State party to the Convention for a dispute between it and one or more other State parties.

21. On the 11th February 2014, both Avrelia and Raptoria, parties to the CCA Convention, declared by a notice addressed to the Depositary (hereinafter: Declaration) that they recognize as compulsory, *ipso facto* and without special agreement, the jurisdiction of an Arbitral Tribunal, subject to reciprocity.

22. However, Article 26 of the CCA Convention allows that such a Declaration covers all disputes or excludes disputes concerning a State's territorial integrity, national defense, title to sovereignty over land territory, or competing claims with regard to jurisdiction over other areas. In light of this possibility, Raptoria made a reservation and decided to exclude disputes concerning national security questions.

23. A conciliation process between Avrelia and Raptoria started on the 30th of August 2020 to address the ongoing cyber terrorism dispute between them. However, efforts within conciliation were unsuccessful. Therefore, after the conciliation process ended, and without a clear commitment by Raptoria to actively engage in the resolving of the dispute,

Avrelia decided, in line with paragraph 3 of Article 26 of the CCA Convention, to file a request for arbitration. On the 4th of November 2020, Avrelia submitted several cyber security related claims by means of an application to the Registrar of the Court, including claims that:

- the Republic of Raptoria bears international responsibility for disabling internet communications in the Kingdom of Avrelia;
- the Republic of Raptoria caused economic damage to the Kingdom of Avrelia which resulted from the disabled internet communications; and
- the Kingdom of Avrelia bears no international responsibility for the launch of multiple cyber attacks from its territory towards the Republic of Raptoria.

24. Raptoria objected to the request submitted by Avrelia, emphasizing that in its Declaration, Raptoria made a reservation and decided to exclude disputes concerning national security questions. Raptoria further stated that in its opinion, the claims presented by Avrelia certainly can be classified as national security questions.

25. Afterwards, an Arbitral Tribunal was constituted, and the Tribunal shall entertain the statements by both parties to the proceedings between the 21st and 24th of November 2023, whereas:

The Kingdom of Avrelia requests the Tribunal to find that:

i. the Kingdom of Avrelia bears no international responsibility for the launch of multiple cyber attacks from its territory towards the Republic of Raptoria;

ii. the Republic of Raptoria bears international responsibility for disabling internet communications in the Kingdom of Avrelia;

iii. in any case, the Republic of Raptoria is required to compensate for the economic damage to the Kingdom of Avrelia which resulted from the disabled internet communications.

The Republic of Raptoria requests the Tribunal to find that:

i. the Arbitral Tribunal has no jurisdiction in the present case;

ii. in any case, if the Tribunal finds that it has jurisdiction, the Republic of Raptoria requests the Tribunal to find that:

- the Kingdom of Avrelia bears international responsibility for the launch of multiple cyber attacks from its territory towards the Republic of Raptoria;

- the Republic of Raptoria acted in accordance with international law in disabling internet communications in the Kingdom of Avrelia;

- in any case, the Republic of Raptoria is not required to compensate for the economic damage to the Kingdom of Avrelia which resulted from the disabled internet communications.

APPENDIX I: CYBER SECURITY LAW OF THE REPUBLIC OF RAPTORIA

Preamble:

Whereas, recognizing the imperative need to protect the sovereign interests and cyber security of Raptoria, the new government of Raptoria hereby enacts the Cyber Security Law with the intention of safeguarding the nation's critical cyber infrastructure, addressing cyber threats, and ensuring the well-being of its citizens.

Article 1: Establishment of The National Agency for Cyber Security (NACS)

1.1. The National Agency for Cyber Security (NACS) is hereby established as the government agency responsible for cyber security at the national level.

1.2. The NACS shall have the authority to develop and implement policies, strategies, and initiatives aimed at enhancing the cyber security posture of Raptoria.

Article 2: Powers and Authorities of The National Agency for Cyber Security (NACS)

2.1. The NACS shall possess the following powers and authorities:

a. Extrajudicial Investigatory and Prosecutorial Powers: The NACS is granted the extrajudicial authority to investigate and prosecute any case related to cyber terrorism, irrespective of jurisdiction, when such cases pose a threat to the national cyber security of Raptoria.

b. Internet Traffic Monitoring: The NACS is authorized to monitor all outgoing and incoming internet traffic entering Raptoria for the purpose of identifying and mitigating cyber security threats.

c. Internet Sector Shutdown: In cases of imminent and severe cyber terrorism threats, the NACS may, when deemed necessary, exercise the power and ability to shut down the entire sector of Raptoria's internet systems to prevent the spread of cyber terrorism, subject to relevant legal safeguards and oversight.

Article 3: Enhanced Evidence-Gathering Powers

3.1. The government shall have enhanced evidence-gathering powers, including:

a. Preservation Duty: Individuals shall have a legal duty to preserve evidence related to cyber security incidents, as requested by the NACS, to aid in investigations.

b. Seize and Shift Power: The government, through the NACS, may exercise the "seize and shift" power, allowing the seizure of evidence for subsequent examination when conducting inspections related to cyber security investigations.

Article 4: Obstruction, Delay, and False Information

4.1. Any individual who attempts to obstruct, delay, or provide false information during cyber security investigations or refuses to comply with solutions aimed at mitigating cyber security problems shall be subject to harsher civil sanctions, as determined by relevant laws and regulations.

Article 5: Ban on VPNs by Private Individuals

5.1. The use of Virtual Private Networks (VPNs) by private individuals is strictly prohibited, except when authorized by the NACS for specific purposes deemed in the interest of national security. Violation of this provision shall result in legal penalties, including but not limited to fines and restrictions on internet access.

Article 6: Oversight and Accountability

6.1. The NACS shall operate transparently and be subject to appropriate oversight mechanisms to ensure the lawful exercise of its powers and authorities.

6.2. Individuals' privacy and civil rights shall be respected in accordance with existing laws and international standards, and any potential infringement shall be subject to review by competent authorities.

Article 7: Implementation and Enforcement

7.1. This Cyber Security Law shall come into effect upon its enactment.

7.2. The government shall take all necessary measures to implement and enforce this law, including the allocation of appropriate resources and the development of regulations and procedures as required.

Article 8: Review and Amendment

8.1. This Cyber Security Law shall be subject to periodic review and amendment, as necessary, to adapt to evolving cyber security challenges and to align with international best practices while safeguarding national interests.

This Cyber Security Law is hereby enacted and signed into law on the 8th of June 2020, with the goal of enhancing cyber security and safeguarding the national interests of the Republic of Raptoria.

APPENDIX II: DECLARATION BETWEEN THE KINGDOM OF AVRELIA AND THE REPUBLIC OF RAPTORIA

This Declaration was entered into on the 11th February 2014 between The Kingdom of Avrelia (hereinafter: Avrelia) and The Republic of Raptoria (hereinafter: Raptoria).

Recitals:

WHEREAS, Avrelia and Raptoria (collectively referred to as the "Parties") have a history of cooperation and a shared desire to strengthen their relationship;

WHEREAS, Avrelila and Raptoria have a desire to solve their possible disputes peacefully and are therefore signing this Declaration, which outlines dispute resolution procedures;

NOW, THEREFORE, in consideration of the mutual covenants contained herein and the provisions of The Declaration, the Parties agree as follows:

Article 1: Purpose of Cooperation

The Parties shall collaborate to foster mutual understanding, promote peace, and enhance their cooperation in various areas, including trade, security and cultural exchange, as outlined in The Declaration.

Article 2: *Ad hoc* Tribunal

The Kingdom of Avrelia and The Republic of Raptoria agree that any dispute that may arise between the States will be resolved in front of any *ad hoc* arbitral tribunal, whose ruling will be legally binding on the parties.

Article 3: Scope of Cooperation

The scope of cooperation shall encompass the following specific activities, responsibilities, and obligations of each party:

- Bilateral Trade: Both parties shall actively promote and facilitate bilateral trade, including the exchange of goods and services, and shall work to remove trade barriers that may hinder economic cooperation.

- Cultural Exchange: The Parties shall encourage cultural exchange programs, including but not limited to educational and artistic exchanges, to foster mutual understanding and appreciation of each other's culture.
- Security Collaboration: The Parties shall collaborate on matters of mutual security concern, such as intelligence sharing and joint efforts to combat transnational threats.
- Environmental Protection: Both parties commit to cooperating on environmental initiatives, including efforts to address climate change, promote sustainable practices, and protect shared natural resources.
- Research and Development: The Parties may engage in joint research and development projects in areas of mutual interest, with the aim of advancing scientific and technological knowledge.
- Education and Scholarships: The Parties shall explore opportunities for educational partnerships and scholarship programs to enhance academic exchanges and educational opportunities for their citizens.
- Healthcare and Public Health: Cooperation in the field of healthcare shall include information sharing, joint public health initiatives, and collaboration on healthcare infrastructure development.
- Humanitarian Aid: In times of crisis or humanitarian need, the Parties shall coordinate their efforts to provide aid and support to affected populations, in accordance with international humanitarian principles.
- Tourism Promotion: Both parties shall jointly promote tourism, encouraging citizens to explore and appreciate the cultural and natural heritage of each other's countries.
- Dispute Resolution: The Parties shall abide by the dispute resolution mechanisms outlined in The Declaration, including the utilization of *ad hoc* arbitral tribunals, as specified in Article 2.

The Republic of Raptoria also recognizes jurisdiction of *ad hoc* tribunals in cases regarding national security questions.

Article 4: Duration of Cooperation

This cooperation shall commence on the Effective Date and continue until otherwise agreed by both parties or until one of the parties submits a resignation letter.

Article 5: Confidentiality

Both Parties agree to maintain the confidentiality of any proprietary or confidential information shared during the course of cooperation, as outlined in The Declaration.

Article 6: Governing Law and Dispute Resolution

The Declaration, including Article 2 thereof, shall govern the resolution of disputes between the Parties, and any disputes arising from this Declaration shall be subject to the dispute resolution mechanisms specified therein.

Article 7: Amendments

This Declaration may only be amended in writing and signed by both Parties, in accordance with the procedures outlined in The Declaration.

Article 8: Entire Agreement

This Declaration constitutes the entire agreement between the Parties and supersedes all prior agreements, understandings, and representations.

Article 9: Execution

This Declaration may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

Article 10: Governing Law and Jurisdiction

This Declaration shall be governed by and construed in accordance with the laws of Avrelia and Raptoria. Any disputes not covered by The Declaration shall be subject to the jurisdiction of the competent courts of the country in which the disputed event happened.

In Witness Whereof, the Parties hereto have executed this Declaration as of the Effective Date.

Signatures:

Party A: The Kingdom of Avrelia

Party B: The Republic of Raptoria

APPENDIX III: DAMAGE ASSESSMENT REPORT

Assessment Report Conducted by: dr. E. W., Senior Analyst of the Avrelian National Security Department

Date of Assessment: 20th of July 2020

Matter: Assessment of the extent of damage caused by the decision of the Raptorian government to temporarily disable all internet connections in Avrelia

Background:

On the 18th of July 2020, the NACS took the unprecedented step of temporarily disabling the entire internet for the Kingdom of Avrelia, which stopped the attack alleged by the Republic of Raptoria.

The sudden and unexpected loss of internet for the entire State caused massive economic damage, as well as a major loss of life for The Kingdom of Avrelia. Raptoria claimed that such a step was necessary to protect their interests and only came as a result of The Kingdom of Avrelia's repeated failure to combat cyber terrorism.

Methodology:

1. **Gathering Information / Data Collection**

The assessment was conducted by gathering information from various sources, including official government statements, independent reports, interviews with affected individuals and businesses, and analysis of economic and social data.

2. **Impact Assessment**

The impact of the internet shutdown was evaluated in terms of economic loss, disruptions to essential services, and the overall effect on the population of Avrelia.

3. **Analysis of Raptoria's Justification**

The basis for Raptoria's decision to disable the internet in Avrelia was scrutinized by examining the claims of repeated failure to combat cyber terrorism and reviewing relevant historical data.

Damage Assessment:

1. **Economic Damage**

The decision to temporarily disable all internet connections in Avrelia resulted in severe economic consequences. Key findings include:

a) **Business Loss**

Businesses across various sectors experienced financial loss due to disrupted operations, inability to conduct online transactions, and supply chain disruptions. Preliminary estimates suggest economic damage of approximately **1.3 billion Euros** to the Avrelian economy.

b) **Unemployment**

The economic downturn led to job loss and a rise in unemployment rates, causing financial hardship for many Avrelians.

2. **Loss of Life and Public Safety**

The sudden internet blackout disrupted several essential services, including emergency response systems, healthcare, and transportation. This disruption had severe consequences:

a) **Loss of Life**

Delayed access to emergency services and medical assistance resulted in a significant loss of life. Conservative estimates indicate that hundreds of lives were lost during the period of internet shutdown.

b) **Public Safety**

The inability to access real-time information and communication channels hindered public safety efforts, leading to an increase in accidents and crimes.

3. **Raptoria’s Justification Analysis**

Raptoria's claim of Avrelia's repeated failure to combat cyber terrorism was examined. While there had been previous cyber incidents, Avrelia has taken several steps to enhance its cybersecurity measures. It is important to note that attributing responsibility for these cyberattacks solely to Avrelia without concrete evidence is a subject of contention.

Conclusion:

The decision by the Raptorian government to disable all internet connections in Avrelia had far-reaching and devastating consequences. The economic loss, loss of life, and disruption of essential services cannot be underestimated.

The claim of Avrelia's repeated failure to combat cyber terrorism, while a serious concern, should be substantiated with concrete evidence before such drastic measures are taken. The internet shutdown inflicted disproportionate harm on the population of Avrelia, and alternative strategies for addressing cyber threats should be explored with a focus on international cooperation and diplomacy.

Immediate efforts should be directed towards restoring normalcy and facilitating diplomatic dialogue to resolve the underlying issues between Raptoria and Avrelia.

APPENDIX IV: RESPONSE OF THE REPUBLIC OF RAPTORIA TO THE DAMAGE ASSESSMENT REPORT ISSUED ON THE 20th of July 2020

Issued by: The Ministry of Foreign Affairs of the Republic of Raptoria

Date: 21th of July 2020

Introduction

While we appreciate dr. E. W.'s assessment of the impact of our decision to disable all internet connections in Avrelia, and respect her expertise, we fundamentally disagree with several key points and conclusions pointed out in her assessment.

Internet Shutdown Justification

The Necessity for National Security: Dr. E. W.'s report questions the necessity of our decision to disable the internet in Avrelia. We assert that this step was taken to protect our national security interests, which were gravely threatened by repeated cyberattacks originating from within Avrelia. The decision was made as a last resort after exhausting all other viable options.

Attribution of Cyberattacks: The report suggests that attributing the cyberattacks solely to Avrelia is subject to contention. We stand by our assertion that extensive intelligence and analysis have confirmed the origin of these attacks. While we respect due process and international standards for evidence, we took action to mitigate the immediate threat posed by these attacks.

Economic and Humanitarian Impact

Economic Loss: We acknowledge the economic loss in Avrelia as a result of the internet shutdown. However, we must emphasize that this loss pales in comparison to the potential devastation that could have occurred if the cyberattacks on our national defense infrastructure had succeeded. Our priority is to protect our nation's vital interests.

Loss of Life and Public Safety: We deeply regret any loss of life and disruption of public safety that resulted from the internet shutdown. It was not our intent to harm innocent civilians, but rather to safeguard our nation from a grave and immediate threat. The blame for these consequences should be placed on the perpetrators of cyberattacks.

International Cooperation

Diplomatic Efforts: We remain open to diplomatic dialogue and international cooperation to resolve the issues between Raptoria and Avrelia. We believe that addressing the root causes of cyber threats requires concerted efforts from both nations and the international community.

Alternative Strategies: We are willing to explore alternative strategies to address cyber threats, but these discussions must be predicated on a genuine commitment from Avrelia to improve its cybersecurity measures and dismantle the networks that facilitate cyberattacks.

Conclusion

In conclusion, while we appreciate Dr. E. W.'s assessment, we firmly reject the findings presented therein. Our decision to disable the internet in Avrelia was driven by a compelling need to protect our national security interests. We remain committed to safeguarding our nation from cyber threats and are open to diplomatic solutions to resolve the ongoing crisis.

We urge the international community to recognize the gravity of the situation and support our efforts to address cyber terrorism: a threat which endangers not only Raptoria, but also global stability and security.