Stockholms universitet

National Cyber Security Strategy for Plutonia

A NCSS for the fictional country of Plutonia as part of the CYBER VT24 course at Stockholm University

Created by Group 13:
Fernando Manuel Sanfeliz (fesa6676@student.su.se)
Gustav Mönefors (gumo9296@student.su.se)
Daniel Nils Braun (dabr4003@student.su.se)
Silas Pohl (sipo6151@student.su.se)

May 14, 2024

Table of Contents

1 Introduction

1.1 Motivation

Plutonia, a Southern European nation, faces a confluence of geopolitical complexities, economic aspirations, and technological advancements, necessitating a robust National Cyber Security Strategy (NCSS). This document outlines the rationale, objectives, and strategic initiatives for developing and implementing a tailored NCSS for Plutonia. With critical sectors increasingly reliant on digital technologies, cybersecurity awareness, public-private collaboration, and innovation are paramount. By uniting government, industry, academia, and civil society, Plutonia aims to mitigate risks, capitalize on digital opportunities, and emerge as a resilient digital ecosystem poised for sustainable growth and global leadership in cyberspace. The structure of this NCSS is based on ITU's "Guide to Developing a National Cybersecurity Strategy" [1] and ENISA's "National Cyber Security Strategies: Practical Guide on Development and Execution" [2].

1.2 Current National Cybersecurity Landscape

Understanding Plutonia's cybersecurity landscape is critical to creating an effective national cybersecurity strategy. Located in Southern Europe, Plutonia faces external geopolitical complexities due to neighboring NATO bases and proximity to influential superpowers, requiring vigilance against potential cyber threats. While Plutonia has a diverse infrastructure, uneven Internet connectivity and the lack of a coordinated national cybersecurity strategy leave critical sectors vulnerable to cyber-attacks that could disrupt essential services and economic operations. Plutonia's democratic governance structure has made progress in reducing corruption. However, the lack of specific cybersecurity legislation poses challenges to enforcing data protection and privacy regulations, particularly in sectors such as healthcare. Plutonia faces cyber threats primarily from organized crime activities. Despite cooperation with international law enforcement agencies, strengthening domestic capabilities is essential to effectively counter emerging cyber threats. Plutonia's education system lacks an emphasis on cybersecurity education and awareness, exacerbating vulnerabilities. Addressing this gap, and tapping into the potential talent pool offered by the somewhat high unemployment rate, is critical to improving cyber resilience. Cyberattacks targeting critical sectors pose a significant threat to Plutonia's economy, underscoring the importance of protecting digital assets and promoting sustainable economic development through robust cybersecurity measures.

1.3 Business Sectors and Services in Scope

Plutonia's NCSS is tailored to address the specific challenges and vulnerabilities present in the nation's unique context. The following sectors and services are identified as key drivers to fulfill the vision:

1. **Critical Infrastructure:** Given Plutonia's reliance on vital sectors such as energy, transportation, telecommunications, and healthcare, safeguarding critical infrastructure against cyber threats is paramount.
2. **Government and Public Services:** Protecting government systems, administrative functions, and public services is essential for maintaining effective governance and upholding national sovereignty.
3. **Financial Sector:** With Plutonia's financial sector serving as a key driver of economic growth and stability, securing banking, insurance, and investment services is imperative.
4. **Healthcare:** Protecting healthcare systems and patient data is critical for ensuring the delivery of quality healthcare services and safeguarding public health.
5. **Education and Research:** Plutonia's education and research institutions play a vital role in knowledge creation, innovation, and intellectual property development.

While the NCSS prioritizes the aforementioned sectors, it also recognizes the importance of cybersecurity across various other areas, including sectors like private enterprise, manufacturing/industrial sectors and transportation/logistics. Plutonia remains committed to addressing cybersecurity challenges holistically, leveraging a multi-sectoral approach to protect digital assets, promote innovation, and safeguard national interests.

2 Vision and Objectives

Vision: Promote a secure, resilient, and innovative digital ecosystem that protects Plutonia's sovereignty, economy, and societal well-being, ensuring trust and prosperity in the face of evolving cyber landscapes and geopolitical complexities.

Objectives:

1. **Enhance Cyber Resilience and Preparedness:**
   Given Plutonia's strategic geographic location and the presence of neighboring NATO bases and potential external threats, strengthening cyber resilience is essential. By investing in proactive measures such as threat intelligence gathering, incident response planning, and robust cyber defense mechanisms, Plutonia can mitigate the impact of cyber incidents and ensure the continuity of critical services.
   - *Impact on Economy:* Protect critical services, ensuring business continuity and economic stability.
   - *Impact on Critical Infrastructure:* Safeguard essential services, minimizing disruptions to citizens' daily lives.
2. **Strengthen National Cyber Defense Capabilities:**
   Due to the prevalence of organized crime activities such as arms and drug smuggling, coupled with the proximity of superpower nations, it is important to enhance cyber defense capabilities. Plutonia must strengthen its cyber defense infrastructure, including the military, law enforcement, and critical infrastructure sectors, to protect against cyber threats to national interests.
   - *Impact on Sovereignty and National Security:* Protect against external threats, safeguarding national interests and strategic assets.
   - *Impact on Military and Law Enforcement:* Ensure the integrity of defense and law enforcement operations, protecting public safety.
3. **Promote Cybersecurity Awareness and Education:**
   With moderate education levels and somewhat high unemployment rates, promoting cybersecurity awareness and digital literacy is imperative. By equipping citizens with the knowledge and skills to identify and mitigate cyber risks, Plutonia can strengthen its overall cyber resilience, reduce vulnerabilities, and mitigate the impact of cyber threats on individuals, businesses, and the economy.
   - *Impact on Citizens:* Empower citizens to protect themselves and their assets, fostering socio-economic well-being.
   - *Impact on Healthcare:* Mitigate risks to patient data, ensuring privacy and safety in healthcare.
4. **Foster Public-Private Partnerships:**
   In a landscape marked by a tradition of corruption and dissatisfaction among some citizens, promoting collaboration between government and private sector entities is essential for effective cybersecurity governance. By establishing public-private partnerships, Plutonia can leverage collective expertise, resources, and information-sharing mechanisms to strengthen the overall resilience of its digital ecosystem.
   - *Impact on Internet Governance and IT Infrastructure:* Strengthen cybersecurity governance and infrastructure, promoting data protection.
   - *Impact on Economic Development:* Drive innovation and economic growth, positioning Plutonia as a cybersecurity hub.
5. **Advance Research and Innovation in Cybersecurity:**
   Given Plutonia's aspirations for economic growth and stability, investing in cybersecurity research and innovation is critical. By fostering an environment conducive to cybersecurity research, development, and innovation, Plutonia can develop a skilled workforce, drive technological advancements, and position itself as a hub of cybersecurity excellence.
   - *Impact on Economic Growth:* Stimulate economic activity and competitiveness, attracting investment and talent.

3 Strategic Priorities

3.1 Protecting Critical Infrastructure

Plutonia will develop a tailored cybersecurity framework leveraging established models (like NIST) to address the unique vulnerabilities of critical sectors like nuclear power plants (given reliance for domestic use and export) and major harbor areas. The framework will encompass sector-specific risk assessments and cybersecurity standards, while incorporating best practices like:

- **Nuclear Power Plants:** Multi-factor authentication, role-based access controls, intrusion detection/prevention systems, and strict vulnerability management.
- **Transportation Systems:** Robust security measures for air traffic control (encryption, access controls), strong protocols for railway signaling, and enhanced security protocols for critical port infrastructure (access controls, network segmentation, intrusion detection).
- **Government Services:** Secure e-government platforms and citizen data with encryption, implement continuous network monitoring, and develop and test incident response plans.

3.2 Stringent Cybersecurity Standards and Regular Audits

Plutonia will establish an independent cybersecurity agency to conduct rigorous audits of critical infrastructure entities, ensuring adherence to national and international cybersecurity standards and promoting continual improvement. Regular audits will enforce mandatory cybersecurity standards tailored to each sector's unique vulnerabilities, with non-compliance addressed through structured penalties and incentives provided for exceeding standards to encourage best practices. To ensure continuous improvement and compliance, a dedicated agency will conduct regular audits of critical infrastructure against national and international cybersecurity standards. Structured penalties will address non-compliance, while exceeding standards will be incentivized. Additionally, mandatory sector-specific standards will be established:

- **Energy Sector:** Regular penetration testing, enforced role-based access control (RBAC), and ongoing security awareness training for personnel.
- **Transportation Sector:** Regular security assessments, implemented encryption protocols, and developed contingency plans for essential operations.
- **Government Services:** Encryption of data at rest and in transit, multi-factor authentication for access, and regular vulnerability assessments with prompt patching.

3.3 Nation Defense and Response

Plutonia will establish Plutonia-CERT as the central command for coordinating national responses to cyber threats and incidents, under the lead national cybersecurity agency. Equipped with advanced technology for monitoring, detecting, and neutralizing threats, Plutonia-CERT will be established with experts from government, private sector, and academia.[1] This team will leverage cutting-edge technology to monitor, detect, and neutralize cyber threats. Plutonia-CERT's core functions encompass:

- **Incident Response:** Providing on-site assistance to critical infrastructure and government agencies during cyberattacks.
- **Investigations:** Leading investigations to understand attack methods, identify attackers, and gather evidence.
- **Threat Intelligence Sharing:** Collecting and disseminating cyber threat intelligence to facilitate proactive defense measures.
- **International Collaboration:** Maintaining communication channels with international CERTs for intelligence sharing and coordinated response to cross-border attacks.

[1] Assumption that cutting-edge technology and sufficient expert resources are available.

Plutonia will implement a comprehensive cyber intelligence strategy to gather and analyze data on potential cyber threats from both domestic and international sources, enabling preemptive actions and policy adjustments. This effort will be supported by a national cybersecurity threat monitoring and response system designed to provide continuous situational awareness and facilitate swift responses to emerging threats. The strategy integrates intelligence from multiple sources including domestic sources (Plutonia-CERT), international partners (CERTs), and private vendors (sector-specific threat feeds). Advanced analytics will identify potential attacks early, enabling proactive measures like issuing threat alerts, network traffic filtering, and disabling vulnerable systems. This national threat monitoring and response system will provide continuous situational awareness and a swift response to cyberattacks.

3.4 Education and Awareness

Plutonia is enhancing cybersecurity awareness across its populace and workforce, to address moderate education levels and high unemployment. The strategy involves a multi-pronged approach:

- **Education Integration:** Cybersecurity education is being integrated at all educational levels: Primary Schools: Teaching basic concepts like password hygiene and safe browsing. Secondary Schools: Expanding knowledge through practical exercises. Higher Education: Offering specialized courses and degrees in cybersecurity.
- **Public Awareness:** Launch nationwide public awareness campaigns utilizing such as TV, radio, and print, alongside social media platforms like Facebook.. These campaigns will educate citizens about preventive practices, recognizing cyber scams, and the importance of cyber hygiene.
- **Collaborations:** Collaborations with civil society and educational institutions to ensure effective communication across all of Plutonian society, fostering a culture of cybersecurity among citizens.

3.5 International Cooperation

Considering its proximity to strategic NATO bases and its EU membership since 2019, Plutonia is committed to strengthening its international cybersecurity alliances to secure its cyberspace comprehensively. This will involve partnering with international organizations like the ITU, OECD, and the Budapest Convention to leverage their expertise, threat intelligence, and capacity-building programs. Additionally, participation in global cybersecurity exercises organized by the ITU and regional bodies will test Plutonia's defenses and foster collaboration with other nations. Furthermore, Plutonia will establish secure communication channels with CERTs in neighboring countries to share cyber threats and coordinate responses to cross-border attacks. This emphasis on global alliances, information sharing, and participation in exercises complements Plutonia's domestic focus on critical infrastructure protection, education, and national defense. This collaborative approach aims to contribute to international efforts in developing global norms and standards for a secure digital environment within Plutonia. Plutonia will regularly engage in international cyber exercises organized by organizations like the ITU and regional bodies to test and enhance its national cyber response capabilities, facilitate collaboration during simulated cyberattacks, and boost preparedness for real-world incidents, both domestically and across borders. This includes establishing secure channels with neighboring CERTs and contributing to international efforts for a more secure digital environment.

4 Governance Structure

4.1 Roles and Responsibilities

Plutonia will establish a central cybersecurity agency to oversee national efforts and coordinate with government departments (transportation, energy) and local governments for a comprehensive national response. This agency will build upon existing structures, assigning clear roles to relevant ministries (defense, education, etc.) and fostering collaboration through a National Cybersecurity Council. The agency will have the following key functions:

- **Strategy and Evaluation:** Overseeing development, implementation, and ongoing assessment of the strategy.
- **Standards and Enforcement:** Creating and enforcing mandatory cybersecurity standards for critical infrastructure.
- **Plutonia-CERT Leadership:** Providing direction to the National Incident Response Team for effective response and intelligence sharing.
- **Public-Private Partnerships:** Collaborating with the private sector to strengthen national cyber resilience.

The leading cybersecurity agency will be staffed with cybersecurity professionals with experience in government, critical infrastructure protection, and incident response.

4.2 Resource Allocation

Plutonia will allocate a significant portion of the national budget to cybersecurity, covering technology upgrades, training programs, and public awareness campaigns to support the implementation of the National Cybersecurity Strategy (NCSS) and sustain ongoing cyber defense efforts.

- **Government Funding:** Allocate government funds to relevant ministries for specific initiatives (i.e leading cybersecurity agency and the Ministry of Education.
- **Public-Private Partnerships:** Explore co-funding with critical infrastructure companies.
- **International Grants:** Investigate international grants for specific cybersecurity projects (i.e ITU).

Plutonia will implement recruitment strategies to attract cybersecurity professionals, who'll be supported by ongoing training and professional development programs to ensure work proficiency, to staff the central cybersecurity agency. A national skills assessment will be conducted to address the workforce in cybersecurity. Moreover, to attract top talent, benefits and competitive salaries will be offered.

5 Risk Management

To identify Plutonia's cybersecurity risks, a SWOT analysis should be conducted. This will highlight the country's cybersecurity strengths and weaknesses, providing a clear picture of areas for quick improvement and those needing more focused effort. Plutonia's advanced technology with widespread 4G, 5G in the capital, and ADSL in rural areas, along with five internet providers, reduces the risk of total internet shutdown if one provider fails.

However, the absence of a domestic Internet Exchange Point, relying instead on external points in the Mediterranean and an eastern neighbor, poses a significant risk. Damage to these points could disrupt the internet, severely impacting critical sectors like healthcare, education, and communication in Plutonia. With the geographical location of Plutonia and its proximity to Nato bases and a superpower nation, it is stuck in the middle and needs to be vigilant for tensions in the area that could potentially lead to cyber espionage or cyber attacks. While an investment in an internet exchange point would be costly at first, it's a long term investment that can improve self reliance of the country's internet, reduce latency, improve control of the routing of data and limit risks of disturbances to it.

With the geographical location of Plutionia and it not being a strong military force, collaboration with EU, Enisa and Nato is very important in order to mitigate risk of conflict and cyber warfare. By engaging in partnership with these organizations Plutonia can get informed of potential cyber threats and how to strengthen its security posture.

6 Monitoring and Evaluation

The ultimate goal of the NCSS is to aid Plutonia and avert national crises. Should cyber threats occur, the strategy needs to be well established and ready to handle any problems. But in order to improve the NCSS it needs to be constantly improved to provide the best possible protection for Plutonia's inhabitants.

The NCSS should be regularly reviewed with an interval of three years for full assessments. Additional audits should be conducted upon major incidents in the world. Participants for such reviews should include the main stakeholders from the public areas government and academia as well as private areas. Public-private partnerships will help realize the review process in an efficient manner. There are two specific current projects that should be closely observed. First, the test phase of the digital hospital journal system. After the test phase, the system's cybersecurity aspects should be evaluated.[2] Second, the development of 5G. Protective security measures should be audited according to state regulations.[3]

To uphold the effectiveness of the NCSS, structures of accountability need to be in place. To prevent conflicts of interest during evaluation and monitoring, the public and private sector need to cooperate. Furthermore, cooperation with Europol and Interpol should facilitate information sharing to profit from a shared pool of knowledge. Additional contact with the civil contingency agency will provide insights in current ongoing events.

7 Legal and Compliance

In alignment with the preventive function of the NCSS, certain areas of law and other legal regulations need to be further examined. To support the NCSS, reforms for strengthening the protection of critical infrastructure are to be done. New legislation should be introduced to improve cybercrime investigation and prosecution capabilities. Additionally, an appropriate legal framework for data protection and privacy should be established. A Cybersecurity Compliance Act[4] will enforce mandatory compliance in the public sector as well as providers of critical infrastructure to improve resilience. The voluntary compliance of the private sector is promoted with incentives for strong cybersecurity practices.

8 Conclusion

The NCSS for Plutiona effectively addresses the nation's specific challenges through a focused approach on objectives, initiatives and responsibilities of key sectors and services to enhance cyber resilience and thus get a step closer to the vision that was agreed upon. The strategy emphasizes the critical role of cyber defense capabilities, public-private partnerships, security awareness among the citizenry and innovation in the area of cyber security.

A multi-pronged approach will be implemented to secure various aspects of Plutonia's framework, such as consideration of citizens' well-being, critical infrastructure, and national defense. This involves improving the education system and increasing awareness, fostering beneficial international relationships, and the creation of a central cybersecurity agency. A risk management analysis shows Plutonia's reliance on external internet exchange points and proximity to geopolitical tensions heightens cybersecurity risks. This requires strategic investments and international collaboration to improve security. International collaboration is key, leveraging global insights and support to enhance Plutonia's cyber defense capabilities. These points reflect Plutonia's strategic direction in cybersecurity, focusing on resilience, collaboration, and continuous improvement to protect its digital ecosystem. With the help of dedicated review mechanisms the NCSS can be continuously monitored and improved. Appropriate legal frameworks will help enforce the compliance of organizations.

[2] Assumption that no documents detailing this plan exist.
[3] Assumption that such a document exists in legislation.
[4] Assumption that such an act doesn't already exist.

References

[1] International Telecommunication Union (ITU), "Guide to Developing a National Cybersecurity Strategy", 2018.

[2] European Network and Information Security Agency (ENISA) "National Cyber Security Strategies: Practical Guide on Development and Execution", 2012.