National Cyber Security Strategy (NCSS) of Plutonia (2024-2029)

Group-14

Group members

Muhammad Aqib
Samir Hossain Santo Bepu
Pavan Gupta
Khondaker Refai Arafat
Faizan Ahmed

Executive Summary

Plutonia's National Cyber Security Strategy (NCSS) outlines a comprehensive vision to establish a secure, resilient, and inclusive digital society by 2034. This strategy aligns with the ITU National Cyber Security Strategy Guideline and prioritizes collaboration between government, critical infrastructure sectors, and the private sector. The NCSS emphasizes the importance of effective governance, legislation, technical measures, and a skilled workforce to achieve cyber resilience. Key objectives include:

- Establishing a National Cyber Security Council (NCSC) and developing a National Cyber Security Policy (NCSP) to provide strategic direction and a comprehensive framework.
- Implementing mandatory cyber security standards for critical infrastructure sectors and essential government services.
- Fostering a culture of cyber security awareness among citizens and businesses.
- Building a skilled cyber security workforce through training programs and capacity building initiatives.
- Enhancing international cooperation through information sharing, participation in international forums and review for adaptation on newly found any cyber threats.

By achieving these objectives, Plutonia can safeguard its critical infrastructure, businesses, and citizens in the digital age.

Table of Contents

1. Introduction

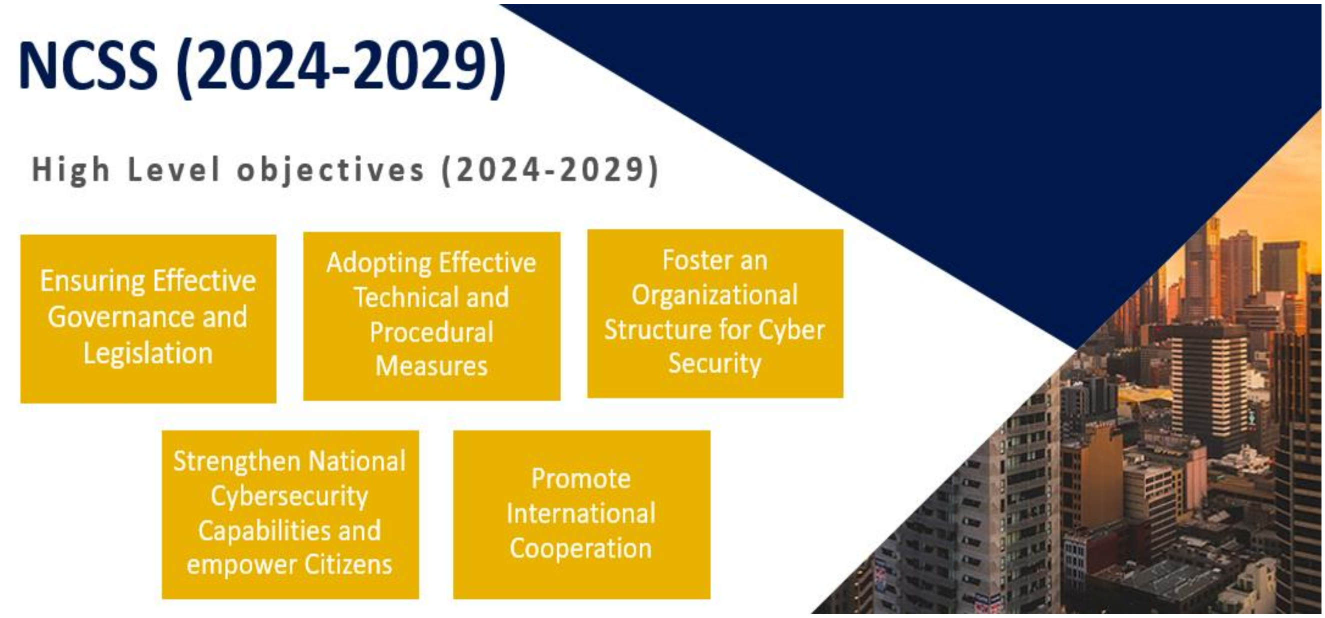
The digital age presents both immense opportunities and significant challenges. While technology fuels innovation and economic growth, it also creates vulnerabilities that cybercriminals can exploit. To connect the full potential of the digital revolution while mitigating cyber risks, Plutonia requires a robust National Cyber Security Strategy (NCSS). This strategy, aligned with the ITU National Cyber Security Strategy Guideline, outlines a comprehensive approach to building a secure, resilient, and inclusive digital society by 2034.

This document details Plutonia's NCSS, encompassing high-level objectives, strategic approaches, and specific actions for various sectors. It emphasizes collaboration between government, critical infrastructure operators, the private sector, and citizens to create a collective defense against cyber threats. By implementing this strategy, Plutonia can safeguard its critical infrastructure, businesses, and citizens in the digital age and foster a thriving digital ecosystem for all.

2. Strategic National Vision on Cyber Security

Plutonia aims to be a leading example of a secure, resilient, and inclusive digital society by 2034. We will achieve this by fostering a collaborative national effort that strengthens critical infrastructure, empowers citizens with cyber awareness, and leverages innovation to build a robust national cyber defense ecosystem.

3. High-Level Objectives (2024-2029)



NCSS (2024-2029)

High Level objectives (2024-2029)

Ensuring Effective Governance and Legislation

Adopting Effective Technical and Procedural Measures

Foster an Organizational Structure for Cyber Security

Strengthen National Cybersecurity Capabilities and empower Citizens

Promote International Cooperation

3.1. Ensuring Effective Governance and Legislation:

The ITU National Cyber Security Strategy (NCSS) Guideline emphasizes the importance of robust governance and legislation to create a secure and resilient digital environment [1,2,6].

3.1.1. Threat Landscape and Considerations:

Plutonia faces a lack of extensive experience in cyber security governance compared to more developed nations. Addressing potential remnants of past corruption is crucial to build trust and transparency in cyber security governance. Aligning Plutonia's cyber security legislation with existing EU regulations ensures consistency and facilitates collaboration within the European Union.

3.1.2. Strategies:

a. **Establish a National Cyber Security Council (NCSC):**
The NCSC will be a high-level body responsible for providing strategic direction, coordinating cyber security efforts across government agencies, and collaborating with stakeholders [1,2]. Its composition should include representatives from relevant ministries (Military Defense, Interior, Justice, Finance), critical infrastructure sectors and cyber security experts. The NCSC will report directly to the Prime Minister or President, ensuring its authority and effectiveness.

b. **Develop a National Cyber Security Policy (NCSP):**
The NCSP will be a comprehensive document outlining Plutonia's cyber security goals, objectives, and implementation plans for the next 5-10 years [1]. It will be aligned with EU directives such as the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR), ensuring compliance and facilitating cooperation with other EU member states [6]. The NCSP should address key areas like cyber risk management, incident response, cybercrime investigation, and international collaboration.

c. **Review and Update Cybercrime Legislation:**
Plutonia's existing cybercrime legislation needs to be reviewed and updated to address emerging cyber threats and align with international standards set by organizations like the Council of Europe's Convention on Cybercrime [6]. Collaboration with international law enforcement agencies like Europol and Interpol can assist in this process.

3.1.3. Implementation Considerations:

Provide training for law enforcement agencies, judiciary, and relevant government officials on handling cybercrime investigations and prosecutions. Allocate necessary resources to establish and maintain the NCSC, develop cyber security policies, and implement new legislation.

3.2. Adopting Effective Technical and Procedural Measures

It encompasses implementing technical controls, establishing best practices, and fostering a proactive approach to cyber security [1,2,4,6].

3.2.1. Threat Landscape and Challenges:

Plutonia has inexperienced and undeveloped cyber threat intelligence capability, making it difficult to anticipate and prepare for emerging threats. Critical infrastructure operators might be reliant on outdated IT systems with known vulnerabilities. Businesses and citizens may lack awareness of best practices like strong password management and secure browsing habits.

3.2.2. Strategies:

a. Develop a National Cyber Threat Intelligence Platform:
Establish a central platform for collecting, analyzing, and sharing cyber threat intelligence across government agencies and critical infrastructure operators. This will enhance situational awareness and facilitate proactive threat mitigation strategies.

b. **Implement Mandatory Cyber Security Standards:**
Define and enforce mandatory cyber security standards for critical infrastructure sectors like energy, finance, healthcare, transportation, and telecommunications. These standards should address secure system configurations, incident response procedures, and vulnerability management practices.

c. Modernize National IT Infrastructure:
Invest in modernizing Plutonia's national IT infrastructure with security in mind. This should include adopting secure coding practices, network segmentation and robust encryption solutions.

d. **Incident Response Planning:**
Develop and implement a national cyber incident response, like CSIRT (Cyber Security Incident Response Team) or CERT (Computer Emergency Response Team), plan outlining roles, responsibilities, and communication protocols for coordinated response efforts to major cyberattacks [1,2,3,4,6].

3.2.3. Implementation Considerations

- Provide training for IT personnel in government agencies and critical infrastructure sectors on implementing and maintaining cyber security measures.
- Allocate necessary resources for developing the cyber threat intelligence platform, establishing cyber security standards, and upgrading national IT infrastructure.
- Allocate sufficient financial resources for the development and implementation of technical controls, infrastructure upgrades, and staff training.

- Regularly review and update technical measures and security practices to adapt to evolving cyber threats.

3.3. Foster an Organizational Structure for Cyber Security

The ITU NCSS Guideline emphasizes the importance of a well-defined organizational structure for cyber security. This structure ensures clear lines of responsibility, facilitates coordination between different stakeholders, and allows for efficient response to cyber threats [1,2].

3.3.1. Threat Landscape and Challenges:

Plutonia is novice with unstructured Government ministries, public services, and private domestic companies especially in the field of IT and Cyber security. It has specific needs and vulnerabilities, weakness of overall national cyber posture.

3.3.2. Strategy and Implementation Considerations for Organizational Structure:

a. **Centralized Coordination:**
Establish a central cyber security authority or agency with the responsibility for developing national cyber security strategy, coordinating cyber security activities across government sectors, essential government services (E-government) and fostering collaboration with private industry and civil society.

b. **Sector-Specific Responsibilities:**
Assign clear cyber security responsibilities to relevant government ministries and agencies overseeing critical infrastructure sectors like energy, transportation, telecommunications, healthcare, and finance.

c. **Public-Private Partnerships (PPP):**
Establish formal mechanisms for collaboration between government and private sector stakeholders. This could involve advisory boards, information sharing platforms, or joint cyber security exercises.

3.4. Strengthen National Cybersecurity Capabilities

3.4.1. Threat Landscape and Challenges:

Plutonia might lack a skilled workforce in cyber security, hindering its ability to effectively monitor, detect, and respond to cyber threats. Citizens might lack basic cyber hygiene practices, making them vulnerable to social engineering attacks and online scams.

3.4.2. Strategies:

The ITU NCSS Guideline recommends the following strategies for Plutonia to address these challenges and strengthen its national cyber security capabilities [5]:

a. **Developing National Cyber Security Infrastructure:**
Invest in modern cyber security technologies like intrusion detection and prevention systems (IDS/IPS), secure network segmentation and data encryption to protect critical national infrastructure.

b. **Empowering Citizens with Cyber Literacy:**
Develop and implement national awareness campaigns and educational programs targeting citizens at all levels, promoting digital literacy and responsible online behavior. Ensure these programs cater to diverse demographics and accessibility needs, creating a more inclusive cyber security culture.

c. **Building a Skilled Workforce:**
Invest in training programs for government officials, law enforcement agencies, and IT professionals to develop specialized cyber security skills, including threat detection, incident response, and digital forensics.

3.4.3. Implementation Considerations:

- Collaborate with private companies, educational institutions, communities and civil society organizations to leverage expertise for awareness campaign programs and training initiatives effectively.
- Utilize various communication channels, such as social media, public service announcements, and community outreach programs, to reach a wider audience and different demographics.
- As cyber threats evolve constantly, therefore, Plutonia should emphasize continuous learning and awareness campaigns to keep citizens informed.

3.5. Promote International Cooperation

3.5.1. Threat Landscape and Challenges:

Plutonia has not strong relationships with other countries and international cyber security organizations. Differences in legal frameworks and information sharing protocols between countries could hinder collaboration and timely threat intelligence exchange. Absence of bilateral agreements with key partners hinders information sharing and joint cyber security exercises.

3.5.2. Strategies for Implementation:

a. **Active Participation in International Forums:**
Participate actively in international cyber security forums like the ENISA (European Union Agency for Cybersecurity), and the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). Engage in discussions, share best practices, and learn from other countries' experiences [4].

b. **Bilateral Cyber Security Agreements:**
Establish bilateral cyber security agreements with key partner countries. These agreements can facilitate information sharing, joint cyber security exercises, and mutual assistance in responding to cyber incidents.

c. **Collaboration with International Law Enforcement Agencies:**
Cooperate with international law enforcement agencies like Europol and Interpol to track down cybercriminals operating across borders. Share information on cybercrime trends, malware analysis, and cybercriminal tactics.

4. Scope of NCSS: Critical Infrastructure Sectors and Business Services (ITU-Aligned)

Plutonia's NCSS should prioritize critical infrastructure sectors and their associated businesses and services. This ensures a comprehensive approach to cyber defense, protecting not only government systems but also the vital services, citizens and businesses rely on.

4.1. Energy Sector:

Sub-sectors: Nuclear power plants, power grids, fuel, transportation companies.

Businesses and Services: Electricity generation, distribution companies, fuel refining and public transportation.

Focus Areas:

- Develop mandatory cyber security standards for critical infrastructure, aligned with international best practices.
- Foster collaboration between government and energy companies to share threat intelligence, conduct joint cyber security exercises, and develop sector-specific cyber security training programs.

4.2. Transportation Sector:

Sub-sectors: Airports, ports, railways.

Businesses and Services: Airlines, air traffic control systems, port operators, shipping companies, railway operators.

Focus Areas:

- Conduct thorough cyber security risk assessments for each transportation sub-sector, identifying vulnerabilities and prioritizing mitigation strategies.
- Encourage the adoption of secure communication protocols, data encryption technologies, and vulnerability management programs across transportation systems.
- Develop comprehensive cyber incident response plans outlining roles, responsibilities, and communication protocols for all stakeholders involved in the transportation sector.

4.3. Telecommunications Sector:

Businesses and Services: Internet Service Providers (ISPs), mobile network operators, data center operators.

Focus Areas:

- Establish and enforce mandatory cyber security standards for ISPs and mobile network operators.
- Encourage collaboration between telecommunication companies, vendors and government agencies to develop national cyber threat intelligence platforms for real-time information sharing.

4.4. Healthcare Sector:

Businesses and Services: Hospitals, clinics, health insurance companies, pharmaceutical companies.

Focus Areas:

- Implement comprehensive cyber security awareness and training programs for healthcare professionals, educating them on data protection regulations, best practices for handling patient information, hospital information systems, including access controls, data encryption, and regular backups.
- Implement HIPAA (Health Insurance Portability and Accountability Act) like federal law of national standards to protect sensitive patient health information.

4.5. Financial Services Sector:

Businesses and Services: Banks, insurance and leasing companies, investment firms, payment processors.

Focus Areas:

- Develop and implement a robust regulatory framework for cyber security in the financial services sector. This framework should include mandatory cyber security standards for financial institutions, focusing on secure online banking systems, multi-factor authentication protocols, data breach notification procedures, and penetration testing requirements.
- Launch public awareness campaigns to educate consumers about online financial scams, phishing attacks, and best practices for secure online transactions.

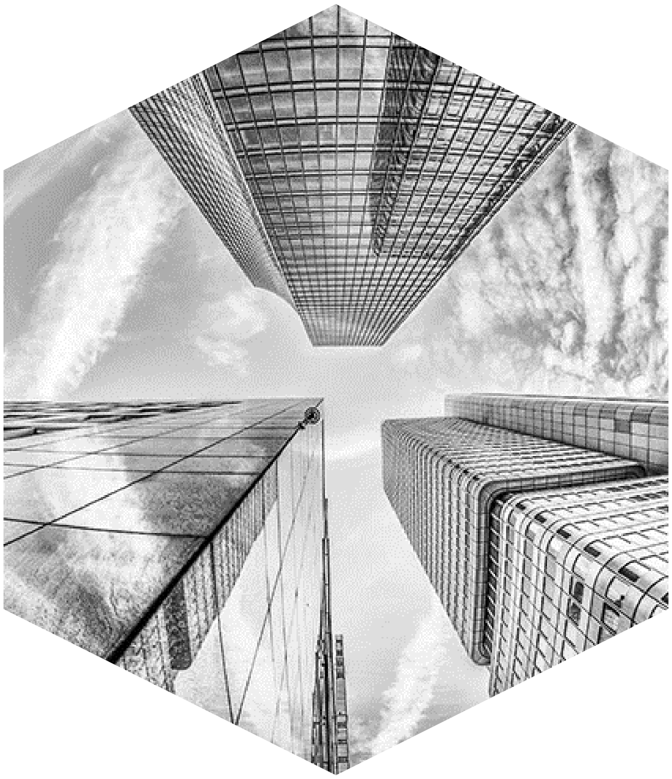
4.6. E-commerce & Other Online Business Services:

Businesses and Services: Online retailers, financial service providers, social media platforms, data storage providers.

Focus Areas:

- Offer tax breaks or financial grants to encourage e-commerce businesses and online service providers to implement robust cyber security measures.
- Implement regulations and policies that protect consumers from online fraud, data breaches, and cybercrime.

5. Scope of NCSS: Government Sectors and Services (ITU-Aligned)



Plutonia's NCSS should extend its scope beyond traditional critical infrastructure to encompass essential government sectors and services. This holistic approach ensures a comprehensive cyber defense strategy protecting not only physical infrastructure but also the digital services citizens and businesses rely on daily.

5.1. National Security:

Focus Areas:

- Implement robust cyber security measures for government networks, including secure access controls, data encryption, and intrusion detection/prevention systems (IDS/IPS).

- Foster collaboration between government agencies and relevant stakeholders (e.g., critical infrastructure operators) to share threat intelligence and best practices.
- Develop a skilled cyber security workforce within government agencies to address cyber threats proactively.

5.2. Public Safety:

Focus Areas:

- Enhance the cyber resilience of emergency response systems (e.g., calling 911) to ensure uninterrupted communication during cyber incidents.
- Train law enforcement personnel in cybercrime investigation techniques to effectively combat cyberattacks targeting public safety.
- Educate citizens about cyber threats and best practices for reporting suspicious activity online.

5.3. Emergency Response:

Focus Areas:

- Develop comprehensive cyber incident response plans for emergency response agencies (like CSIRT, CERT) outlining actions to take during an attack and communication protocols for all stakeholders [1,2,3,4,6].
- Implement robust backup and recovery procedures for critical emergency response data to ensure rapid restoration of services in case of a cyberattack.

5.4. E-Government Services:

Focus Areas:

- Develop and maintain secure online platforms for citizen interaction with government services, including strong user authentication protocols and data encryption.
- Implement robust vulnerability management programs to identify and address vulnerabilities in e-government platforms swiftly.
- Maintain transparency with citizens regarding cyber incidents affecting e-government services and communicate mitigation efforts effectively.

6. Specific Objectives and Priority

Impact Area	**Objective**	**Timeline (years)**	**Priority**
Economy	Increase the cyber maturity of critical infrastructure operators to reduce economic disruptions from cyberattacks.	3	High
Military	Implement a national cyber defense strategy to protect military systems and ensure national security.	2	High

Internet Governance	Develop a national cyber security framework that promotes a secure and open internet environment.	2	High
IT Infrastructure	Invest in secure and resilient IT infrastructure for both public and private sectors.	5	High
Healthcare	Implement strong cyber security measures to protect sensitive patient data and ensure the continued operation of healthcare systems.	3	Medium
Citizens	Enhance public awareness and education on cyber security best practices.	3	Low

Prioritization Rationale:

High Priority: Objectives critical to protecting Plutonia's essential services, national security, and economic well-being.

Medium Priority: Objectives that contribute to a more secure and resilient digital environment and foster a culture of cyber awareness.

Low Priority: Objectives that promote long-term goals but require ongoing efforts and resource allocation.

7. Directive in Future

This strategy provides a high-level roadmap. Further steps include:

- Developing detailed implementation plans for each objective.
- Establishing a National Cyber Security Council for coordination and oversight.
- Allocating resources for capacity building and infrastructure improvements.
- Public awareness campaigns to promote cyber hygiene.
- Adaptive to new threats

8. Conclusion

This National Cyber Security Strategy outlines a comprehensive approach to safeguard Plutonia's digital future. By prioritizing national security, economic development, and citizen empowerment, we can create a resilient and trusted digital space for all.

9. Reference

[1] Eric Luiijf and Kim Besseling, “Nineteen national cyber security strategies”, Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, 2013, https://www.researchgate.net/publication/261950643_Nineteen_National_Cyber_Security_Strategies

[2] H.A.M. Luiijf, Kim Besseling, Maartje Spoelstra, and Patrick de Graaf, “Ten National Cyber Security Strategies: A Comparison”, Critical Information Infrastructure Security, 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, https://link.springer.com/chapter/10.1007/978-3-642-41476-3_1

[3] Dr. Frederick Wamala (Ph.D.), “THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE”, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

[4] Narmeen Shafqat and Ashraf Masood, “Comparative Analysis of Various National Cyber Security Strategies”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 14, No. 1, January 2016, https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies

[5] Richard A.I. Johnson and Max Gallop, “Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies”, Journal of Cyber Policy 7(3):375-398, DOI:10.1080/23738871.2023.2178318, February 2023, https://www.researchgate.net/publication/370979728_Building_cybersecurity_capacity_a_framework_of_analysis_for_national_cybersecurity_strategies

[6] Anna Sarri, Gema Fernández Bascuñana,Ann-Kristin Gross, Federico Chiarelli, Marina Preasca, “A Governance Framework for National Cybersecurity Strategies”, ISBN: 978-92-9204-589-0, DOI: 10.2824/211856, Catalogue number: TP-04-22-152-EN-N, February 2023.