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

NCSS created by:
Fernando Manuel Sanfeliz (xxxxXXXX@student.su.se)
Gustav Mönefors (xxxxXXXX@student.su.se)
Daniel Nils Braun (xxxxXXXX@student.su.se)
Silas Pohl (sipo6151@student.su.se)

May 10, 2024

Table of Contents

1 Introduction

1.1 Motivation

In an era defined by digital interconnectedness, safeguarding national security extends beyond physical borders to encompass the protection of digital infrastructure and sensitive data. 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. Against a backdrop of democratic governance, reduced corruption, and EU membership, Plutonia confronts cyber threats from strategic NATO bases, neighboring superpowers, and a growing digital economy. 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, capitalise on digital opportunities, and emerge as a resilient digital ecosystem poised for sustainable growth and global leadership in cyberspace.

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.

Plutonia's cybersecurity landscape presents challenges that require a strategic and collaborative approach. Addressing vulnerabilities, improving regulatory frameworks, promoting cybersecurity education, and strengthening public-private partnerships are key to protecting national interests and advancing cyber resilience initiatives.

1.3 Vision and Objectives

Vision: Foster a secure, resilient, and innovative digital ecosystem that protects Plutonia's sovereignty, economy, and societal well-being, ensuring trust and prosperity amidst 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, economic activities, and national security operations.

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 and ensure the integrity, confidentiality, and availability of sensitive information and essential services.
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.
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 combat cyber threats, improve incident response capabilities, and increase the overall resilience of its digital ecosystem.
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, staying ahead of evolving cyber threats and ensuring its digital sovereignty and economic prosperity.

1.4 Business Sectors and Servcies in Scope

Plutonia's National Cyber Security Strategy (NCSS) is tailored to address the specific challenges and vulnerabilities present in the nation's unique context. The scope of the NCSS encompasses key sectors and services critical to Plutonia's sovereignty, economic stability, and societal well-being, taking into account the prevailing geopolitical dynamics, infrastructure landscape, and cybersecurity priorities. The following sectors and services are identified as essential within the scope of the strategy:

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 other areas, including 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 in an increasingly interconnected and digitized world.

Appendices

A Appendix Section

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam auctor mi risus, quis tempor libero hendrerit at. Duis hendrerit placerat quam et semper. Nam ultricies metus vehicula arcu viverra, vel ullamcorper justo elementum. Pellentesque vel mi ac lectus cursus posuere et nec ex. Fusce quis mauris egestas lacus commodo venenatis. Ut at arcu lectus. Donec et urna nunc. Morbi eu nisl cursus sapien eleifend tincidunt quis quis est. Donec ut orci ex. Praesent ligula enim, ullamcorper non lorem a, ultrices volutpat dolor. Nullam at imperdiet urna. Pellentesque nec velit eget euismod pretium.

B Appendix Section

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam auctor mi risus, quis tempor libero hendrerit at. Duis hendrerit placerat quam et semper. Nam ultricies metus vehicula arcu viverra, vel ullamcorper justo elementum. Pellentesque vel mi ac lectus cursus posuere et nec ex. Fusce quis mauris egestas lacus commodo venenatis. Ut at arcu lectus. Donec et urna nunc. Morbi eu nisl cursus sapien eleifend tincidunt quis quis est. Donec ut orci ex. Praesent ligula enim, ullamcorper non lorem a, ultrices volutpat dolor. Nullam at imperdiet urna. Pellentesque nec velit eget euismod pretium.

C Appendix Section

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam auctor mi risus, quis tempor libero hendrerit at. Duis hendrerit placerat quam et semper. Nam ultricies metus vehicula arcu viverra, vel ullamcorper justo elementum. Pellentesque vel mi ac lectus cursus posuere et nec ex. Fusce quis mauris egestas lacus commodo venenatis. Ut at arcu lectus. Donec et urna nunc. Morbi eu nisl cursus sapien eleifend tincidunt quis quis est. Donec ut orci ex. Praesent ligula enim, ullamcorper non lorem a, ultrices volutpat dolor. Nullam at imperdiet urna. Pellentesque nec velit eget euismod pretium.