Atlantis Cyber Security Strategy
Group 10

Participants

Athanasios Ntales (atnt3398)

Bilal Riaz (biri9477)

Chanchala Fernando (chfe1432)

Emad Abdulsamad (emab9908)

Lekhaz Adapa (lead3201)

TABLE OF CONTENTS

Introduction

The need for a cybersecurity strategy stem from the fact that digital transformation is an international phenomenon that has an impact on all facets of society and poses both significant opportunities and risks. Our capability to sustain and improve both our prosperity and security is significantly impacted by how well we manage threats and risks associated with digital transformation. The entire society is concerned with cybersecurity, so everyone must bear responsibility for these problems to manage information effectively and securely. The challenges in the field of cybersecurity are shared with other nations, and it is necessary to develop strategic solutions through international cooperation and discussion of preventive measures, both within the EU and in other international organizations. Strong cybersecurity is required for Atlantis' society's growth and competitiveness as well as for the private sector to develop and offer competitive solutions and services considering the escalating demands on society's cybersecurity [1].

Scope

This National Cyber Security Strategy (NCSS) aims to create a framework for enhancing Atlantis, a tiny EU nation in Southern Europe's cyber security posture. Atlantis, with an estimated population of around 15 million people, presents a variety of cyber security concerns that must be solved to secure its residents, businesses, facilities, and economy against ever-expanding cyber-attacks. This NCSS considered current and modern strategies to comply with cyber security strategies in neighboring countries.

The NCSS is predicated on the premise that cyberspace is continually developing and that threats to Atlantis' cyberspace, information systems, and information communication infrastructure are constantly rising. The NCSS will guide Atlantis to be proactive in its cyber security approach to defend the country from possible cyber threats and attacks. The NCSS will also assist Atlantis to meet its strategic objectives and goals by ensuring the ability to develop and maintain a secure, flexible, and reliable cyber environment.

This NCSS attempts to accomplish the following goals:

- Establish an ambitious plan for the next phase of Atlantis' cyber security and set high-level objectives that must be met within a particular time limit.
- Identify the business categories and services the plan covers and describe specific goals for each.
- Prioritize goals depending on their potential societal influence, such as the economy, the military, digital administration, IT infrastructure, healthcare, and citizens.
- Create a governance framework to ensure the NCSS's successful implementation and monitoring.
- Increase the general public's knowledge of cyber security, and ensure every stakeholder is involved in the NCSS implementation.

The NCSS will be evaluated and updated regularly to improve and guarantee its effectiveness and relevance in the face of new cyber security threats and dangers.

Vision

The National Cybersecurity Strategy of Atlantis aims to protect the country against security threats, risks, and challenges to national security by creating a coherent vision for keeping Atlantis prosperous and secure. The strategy sets out a framework for managing cyber threats and protecting critical systems and infrastructure. The threats for cyberattacks on information systems and infrastructure owned by the private sector in the business, industrial, and communications sectors must be managed and patched through public-private collaboration. The primary objectives are to secure information, information systems, and communication systems of the public sector and services against cybercrimes, protect Atlantis' business and citizens by building a cybersecurity frame, secure the use of cyberspace to prevent malicious and forbidden use and establish a framework for international cyberspace security. The NCSS is centered on the International Telecommunication Union guidance and standards to build effective collaboration with other strategies for neighboring countries [2].

High-level objectives

1. Secure information systems and information communication infrastructure against possible threats.
2. Enhance public-private operational collaboration to secure information systems and infrastructure for different private businesses and industrial sectors.
3. Develop and update nationwide incident detection and response plans and processes.
4. Create a governmental agency responsible for establishing, implementing, maintaining, and monitoring cybersecurity strategies and policies.
5. Enhance international cybersecurity cooperation.

Objectives and Priorities

1. Secure information systems and information communication infrastructure against possible threats:

1.1. Secure information and information system:

Establishing and implementing Atlantis information and information systems should include a national model and responsibilities for cyber security and conduct required systematic cyber security efforts to increase the capability to prevent, detect and manage cyberattacks and other security incidents and promote knowledge and expertise. All stakeholders should be involved in establishing and implementing NCSS to have a comprehensive view of cyber security and cover different fields, including technology, administration, economics, and law. Cyber security is to be a natural and integral part of all work at all levels of society within and between organizations and different sectors of society. Security measures should aim to create more effective information management and to manage more serious disruptions and crises.

Robust cyber security is important for all governmental, business, and industrial operations and processes to achieve their quality and effectiveness. Governmental, business, and industrial services flow in several stages, and deficiencies in cyber security can have repercussions far beyond the boundaries of the activity. Therefore, improving cyber security is a requirement, as well as a frequent activity [1].

1.2. Secure Information Communication Systems:

The NCSS provides conditions and procedures for different providers and operators to be applied and followed in all communication operations and processes and to guide stakeholders to secure networks, protect communication infrastructure, and enhance the capability to prevent, detect, and mitigate cyberattacks and other security incidents. The strategy encompasses the whole of society, including central government authorities, municipalities and county councils, companies, organizations, and private individuals. The Atlantic government must enforce robust and effective monitoring systems on all communication systems and communication infrastructure to detect any malicious behavior or attack.

All providers and operators should use cryptographic controls to protect transmitted information and implement an effective monitoring system. Mobile network operators must integrate all 4g and 5g security standards in the implementation of the mobile network [3].

2. Enhance public-private operational collaboration to secure information systems and infrastructure for different private businesses and industrial sectors.

The National Cybersecurity Strategy outlines the objective of enhancing public-private operational collaboration for securing information systems and infrastructure for different private sectors to allow the Atlantis government to scale coordination with critical infrastructure owners and operators across. This objective aims to develop and strengthen collaboration between cyber stakeholders through structured roles and responsibilities and to increase information sharing and connectivity by enabling the automated exchanging of data, information, and knowledge between different parties. The NCSS also emphasizes the need to improve data sharing and security orchestration to enable real-time, efficient, and multi-directional sharing to immediately warn cyber defenders and notify victims and drive required responses for all new upcoming threats and attacks. The Atlantis government provides private sectors with needed technical platforms that allow them to enable continuous, coordinated operations to disrupt malicious activity on a large scale. Additionally, the objective encourages private sector partners to work together and organize their efforts through one or more governmental and nonprofit organizations that can serve as hubs for public-private operational collaboration and ensure the implementation and adaptation of cyber security policies [3].

Society Sectors	CS security policy	Explanation
Economy	1. Establish and execute a national cyber security framework. 2. Support optimal procedures and regulations. 3. Create a legal and regulatory framework. 4. Ensure adopting long-term investing in cybersecurity.	Factors such as economic impact, cost-effectiveness, and alignment with national economics standards and priorities have been considered when prioritizing objectives.
Military	1. Establish and execute a national cyber security framework. 2. Create a legal and regulatory framework. 3. Building a robust and diverse cyber workforce 4. Embracing security and resilience by design	The protection of digital defensive systems is the main factor when considering prioritization in military terms.
Internet governance	1. Establish and execute a national cyber security framework. 2. Create a legal and regulatory framework. 3. Apply a robust and 4. Improve public awareness and education regarding cyber threats and how to guard against them.	The orientation of this prioritization is based on ensuring a secure and sustainable internet ecosystem.
IT infrastructure	1. Support optimal procedures and regulations. 2. Establish and execute a national cyber security framework. 3. Create a legal and regulatory framework. 4. Improve public awareness and education regarding cyber threats and how to guard against them.	Here, what is important is to make sure that the most critical areas are well focused and protected, regarding Atlantis's goals and requirements.
Health care	1. Improve public awareness and education regarding cyber threats and how to guard against them. 2. Support optimal procedures and regulations. 3. Create a legal and regulatory framework.	Patient safety and quality of health care services are factors that prioritization in terms of health care has to consider in order to improve healthcare outcomes.

	4. Increase law enforcement capabilities. 5. Establish and execute a national cyber security framework.	
Citizens	1. Improve public awareness and education regarding cyber threats and how to guard against them. 2. Create a legal and regulatory framework. 3. Support optimal procedures and regulations. 4. Establish and execute a national cyber security framework.	The most important factor in this prioritization is to enhance the quality of citizen's lives by promoting a more citizen-centric approach.

3. Develop and update nationwide incident detection and response plans and processes.

From the perspective of the national cybersecurity strategy of Atlantis, it is essential to take cyber threats and attack considerations into account when creating and updating national incident response plans and procedures. Detection and response planning will be implemented through the following steps to enable incident response processes and plans to be tailored to meet the unique challenges and complexity of cyber security incidents [3].

Firstly, Atlantis should conduct risk analyses, including vulnerability and threat analyses, as well as protective security analyses to identify potential threats and vulnerabilities. Vulnerability and threat analyses and assessments can be used to develop incident response plans and to improve contingency and continuity plans.

Secondly, based on risks and threats, analyses and assessments establish a coordinated approach to incident response and involve all stakeholders with all authorities to implement the decision-making pathways. This requires coordination of competencies and effective communication between all agencies and organizations in all society's sectors.

Thirdly, cyber security training activities should be prioritized to build expertise and guarantee an excellent capability to manage serious IT incidents. This includes long-term planning and coordination to ensure good cyber security knowledge and awareness in order to achieve all the levels and competencies that are needed to manage urgent and severe cyber security incidents.

Finally, Atlantis should continually maintain and improve the capability to manage serious IT incidents and to regularly review and update incident response plans and processes to ensure their efficiency and effectiveness.

4. Create a governmental agency responsible for establishing, implementing, maintaining, and monitoring cybersecurity strategies and policies.
A cyber security agency plays a crucial role in protecting critical infrastructure and systems, establishing regulations, and defending security agencies and national security systems. The agency works to establish regulations that can drive better cybersecurity practices at scale and encourage public-private collaboration and innovation. The agency also works to defend national security systems against a wide range of cyber threats, including insider threats, cybercriminals, and the most sophisticated nation-state adversaries. The agency also works to help and aid recovery in the event of a catastrophic cyber incident. The National Cybersecurity Agency is responsible for establishing, implementing, and improving a proactive and comprehensive national approach to cybersecurity as follows.

4.1. Establish and execute a national cyber security framework: Atlantis will create and implement a national cyber security framework to offer an integrated approach to cyber security throughout all business sectors and services. The structure will determine and tackle cyber security hazards and weaknesses and provide incident recovery and response protocols. In addition, the framework would define roles and duties for various organizations associated with cyber security, such as government agencies, enterprises, and people.

4.2. Increase law enforcement capabilities: Atlantis' law enforcement agencies will create specialist cyber security teams to increase their powers in identifying, investigating, and punishing cyber offenders. Training courses will guarantee law enforcement employees have the skills and information to respond to cyber threats successfully. To enhance law enforcement activities in this area, advanced technology will be purchased.

4.3. Support optimal procedures and regulations: The NCSS intends to motivate organizations and companies in Atlantis to embrace standards and best practices to strengthen their online security posture. Guidelines will be established to assist companies and groups in following these best practices. Certification schemes will be developed to give independent certification that a company or organization has implemented adequate cyber security measures.

4.4. Create a legal and regulatory framework: A legal and regulatory framework will assist the NCSS and allow the government to react effectively to cyber threats. International standards and best practices will develop the framework. It will also define cybercrime sanctions and recommend incident recovery and response. With the legislative and regulatory framework, the government can collaborate with organizations and companies to tackle risks and vulnerabilities.

5. Enhance international cybersecurity cooperation.

Enhancing international cybersecurity cooperation is an essential aspect of the NCSS, especially in the context of Atlantis being an EU member state. As cyber threats are often transnational, it is necessary to collaborate with other countries and international organizations to exchange information, best practices, and technologies to prevent and respond to cyber-attacks.

This objective includes establishing partnerships with other countries, regional organizations, and international bodies to enhance information sharing, joint training and exercises, and capacity-building initiatives. Atlantis may also participate in international forums and conferences to promote cooperation and collaboration on cybersecurity issues.

Moreover, the NCSS may aim to align with international standards and guidelines, such as the NIST Cybersecurity Framework or the ISO/IEC 27001, to ensure consistency and interoperability with other countries' cybersecurity frameworks. This alignment can facilitate international cybersecurity cooperation and strengthen critical systems and infrastructure protection.

Enhancing international cybersecurity cooperation can be instrumental in ensuring a coordinated and effective response to cyber threats that could impact Atlantis, other countries, and the international community [4].

References

[1] Government Offices of Sweden, "A national cyber security strategy", Skr. 2016/17:213, June 2017. Available on: https://www.government.se/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

[2] International Telecommunication Union (ITU), " Guide to Developing a National Cybersecurity Strategy", published in 2018. Available on: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

[3] The White House. Washington, "National Cybersecurity Strategy", March 2023. Available on: https://www.documentcloud.org/documents/23694061-national-cybersecurity-strategy-2023

[4] International Organization for Standardization, "ISO 27001, The International Information Security Standard,", ISO/IEC 27001:2013, published in 2013. Available on: https://www.itgovernanceusa.com/iso27001-and-nist