Atlantis National Cyber Security Strategy *(NCSS)*

Group #10

Table of Contents

I. Introduction

1. Scope

This strategy offers a framework that ought to be carried out by the Cybersecurity Department during the next five years to keep pace with the continuously growing cyber risk. Atlantis' Cybersecurity Department should improve the country's cyber-resilience by working actively on identifying new vulnerabilities, responding to incidents, and countering any malicious actors while improving Atlantis' cyberdefense.

The strategy covers vital, essential, and critical business sectors of varying sizes in the country. At-risk industries that need a maximum level and up-to-date cyber security, which this strategy covers, are government agencies, the military establishment, healthcare organizations, financial and commerce sectors, the power and energy industry, IT and communication infrastructure, transportation, and higher education facilities. Moreover, this strategy aims to protect citizens and residents of Atlantis against cyber threats involving digital data.

2. Vision and Statement of purpose

This document is "The National Cybersecurity Strategy of Atlantis." It provides long-term measures for protecting the country against security threats, risks, and challenges to national security. Through the coordination of government, private sector, citizens and international efforts in cyberspace defense, this document is designed to create a coherent vision for keeping Atlantis prosperous and secure [1].

The National Cybersecurity Strategy sets out a framework for managing cyber threats or protecting our critical infrastructure. To meet the goals, the strategy raises the profile of cybersecurity within our national and regional governments and outlines clear roles and responsibilities for the actors involved in the process. In addition, this Strategy requires a public-private partnership to fix the potential vulnerability of private sector-owned critical infrastructures in the banking, utilities, and telecommunications sectors against cyber attacks [1].

The vision and strategy to implement the NCSS will be centered on the International Telecommunication Union's Global Cybersecurity Agenda (GCA) in order to build an effective collaboration between relevant parties in the joint effort to fight cyber threats. Therefore the aim is to create a secure and safe information society based upon the following pillars [1]:

- Organizational Structures.
- Capacity Building and Citizens protection.
- International Cooperation.

3. Strategic context

With the continuous growth in Internet access and Internet-enabled devices, there has been a massive availability of datasets and a need for high-speed information systems. These would improve productivity, efficiency, and capacities in all different sectors. However, because more devices are now connected to the Internet, there is also a higher risk of cyber-threats.
Many advanced cyberattacks have exposed, encrypted, or damaged sensitive data, causing countries to lose vital services, experience economic loss, and pose national security risks. Cyber threats can be caused by a variety of actors, such as hostile nation-states, hacktivists, criminal organizations, terrorist groups, disgruntled employees, etc. As a result of the inner nature of some threats, national levels of cooperation between entities are called for to be flexible and robust. Meanwhile, the cross-border nature of some threats makes it imperative to plan for active international cooperation to meet new global threats.

In the context of Atlantis, our cyberspace faces a range of different threats. Cyber threats range from espionage directed towards obtaining political intelligence, facilitated by governmental corruption, to phishing attacks aimed to facilitate credit card fraud, identity theft, or other forms of cyberattacks fuelled by the high level of unemployment in the country [1].

Despite the absence of direct internal and external conflicts, the instability of Atlantis' neighbouring countries represents a potential threat that could result in a variety of threats, including manipulation or denial of service attacks against the country's significant infrastructures. Due to the presence of nuclear plants within the country's borders, and given the dependence of the energy sector on cyberspace, protection of such critical infrastructure is a top priority [1].

4. Primary Objectives

Atlantis' National Cyber Security Strategy aims to support and maintain safe cyberspace in which the existence of a highly secure and resilient digital infrastructure can operate with the highest efficiency without jeopardising the rights and freedoms of citizens. Atlantis must strengthen capabilities guided by its national values and laws, taking individuals' privacy into account to guarantee safe and responsible use of information, information systems, and communication networks.

The primary Cyber security objectives:

1. Secure information, information systems, and network systems of the public sector and essential services against cybercrimes in terms of confidentiality, integrity, and availability and ensure their resilience.
2. Protect Atlantis' business and citizens by building a cybersecurity frame and strengthening people's security awareness and skills.
3. Secure the use of cyberspace to prevent malicious and forbidden use.
4. Establish a framework for international cyberspace security.

II. Strategic Pillars

Pillar 1: Organizational Structures

Objective: Atlantis will defend its fundamental interests in cyberspace by managing cybersecurity risks. There will be an increase in the digital security and resilience of Atlantis' critical infrastructure, and information systems.

Measure 1: Secure Information and Control System, which are parts of the critical infrastructure

The emergence of new technologies, such as the Internet of Things (IoT), brings an increase in the number of connected devices in Atlantis. These devices are used in the industrial sector, as well, in critical infrastructure, in order to control and observe physical processes. They may also be called SCADA systems. As they are part of the industrial information and control system, there is a need in maintaining national expertise in this area, which would

lead to improving security. This would prevent Atlantis from any disruptions, which could affect the proper functioning of society. For instance, an attack on the drinking water supply could be a disaster for the country. Furthermore, as IoT devices can also be used in different sectors (e.g., the transport or healthcare sectors), this means that they are also susceptible to be victims of any disruptions. Thus, the government should provide a preventive environment to the different sectors. In order to meet the challenges, a collaborative effort between private, and public sectors should be established, while also, Atlantis should make sure that different companies and authorities have access to developed conditions to improve their cybersecurity resilience. Finally, Atlantis should also incentivize the cybersecurity investment and push the idea of developing locally high-security products, which will contribute to the employment of the country [2].

Measure 2: Give support to the procurement of secure electronic communication and other IT services.

As the demand of accessing the Internet is increasing, there is a need to obtain a high level of operational reliability between different network communications and IT services. This could concern the ability to provide alternative links quickly while also being able to provide an appropriate level of reliability. The government ought to help stakeholders in the sector, to improve their abilities to handle serious disruptions by providing support in purchasing different external electronic communications. This support should also include the different IT services [2].

Pillar 2: Capacity building and Citizen Protection

Objective: All organizations and citizens have the right to use cyberspace securely. To that end, Atlantis has the full responsibility to build, promote, and encourage measures to achieve and maintain sufficient institutional and human cyber defence across all society entities.

Measure 1: Building a skilled cybersecurity workforce of different levels of capabilities and knowledge.

The national security and economic stability of Atlantis depend on having a highly-skilled cybersecurity workforce that keeps the information and systems safe. Developing a cyber workforce requires a strategic approach done by all relevant sectors to identify issues, design and implement security strategy, policies, and procedures, manage costs and consistently evaluate the impact, etc. Others involve designing protection, detection, and response capabilities. The workforce must possess the knowledge and authority to respond to cyber security incidents, verify compliance, monitor, and audit.

Measure 2: Building a national cybersecurity culture and raising security awareness among Atantis's citizens.

Developing a national cybersecurity culture is one of the primary responsibilities of the nation. Atlantis aims to transfer cybersecurity knowledge to all relevant stakeholders involving citizens, which promotes the nation's security posture and plays a significant role in protecting the information and systems. Security awareness campaigns are necessary for the safe use of cyberspace. Developing dedicated academic cybersecurity education and programs and fostering research and development are the nation's goals to supply society with qualified professionals. Moreover, promoting cooperation with academia, the public sector, and the community plays a significant role in building the nation's security culture [1].

Pillar 3: International Cooperation

Objective: In cooperation with voluntary member states, Atlantis will drive the European joint effort against cyber threats, playing a key role in promoting a safe, stable, and open international cyberspace [3].

Measure 1: Establishing a short term agenda to achieve European Strategic autonomy

With the collaboration of voluntary EU member states, Atlantis will develop a common agenda to achieve European digital strategic autonomy. It will be based on enforcing a series of short-term policies to reach common ground among the joining members in terms of regulations, standardization and certification, research and development. Most importantly, this goal will be pursued by keeping the citizens' right to privacy at the forefront.
This measure will allow the states involved to maintain their own sovereignty while strengthening their reciprocal trust in the cybersphere, as well as advancing the effectiveness and security of cross-border communication [3].

Measure 2: Actively contributing to the stability of the global cyberspace by assisting other countries in establishing the necessary cyber-security capabilities

Due to the existence of a global gap between countries' digital advancement and digital transition capabilities, Atlantis will contribute to sharing physical and intellectual resources to facilitate the advancement process for countries willing to agree on a digital partnership with Atlantis. Given the precarious state of the political and economic stability of our neighbouring countries, it is important to contribute with the necessary support in order to

increase the resilience of their critical infrastructures from cyber threats and prevent undesired consequences that may indirectly jeopardise the stability of Atlantis' national cyberspace.

Towards this end, It is preferable for Atlantis to act through long-term, trust-based partnerships to keep projects durable and sustainable. By doing so, Atlantis will also be able to strengthen its own cybersecurity [3].

III. References

[1] ITU. 2011. *ITU National CyberSecurity Strategy Guid*e. International Telecommunication Union, Geneva, Switzerland.

[2] 2017. *A national cyber security strategy*. Stockholm: Government Offices of Sweden.

[3] 2015. *French national cyber security strategy.* Agence nationale de la sécurité des systèmes d'information.