Cyberia’s Cyber Security Strategy

Empowering Innovation and Growth towards Development

Submitted by:

Group 15

Justas, Ranjana, Efstathios

[**EXECUTIVE SUMMARY**](#_3ih8zcfb80xj) **3**

[**CHAPTER 1**](#_bow1q565a0uo) **4**

[OVERVIEW OF CYBERIA](#_824vhd6houy6) 4

[**CHAPTER 2**](#_b0ap5wwj4smj) **5**

[LINE OF ACTION DEFINITION](#_asyqqg6wrxdz) 5

[Vision](#_t3fivdp3rf2) 5

[Objectives](#_y03wcdd9l2ll) 5

[Initiative](#_9ezp80ozfrpe) 6

[**CHAPTER 3**](#_qvje2xqazmmf) **7**

[NEED FOR CYBER SECURITY STRATEGY](#_4dovquwby0qc) 7

[Identification of Critical Infrastructure](#_9fvxgq92rvsx) 7

[Threats](#_47q3w1zhcbgv) 8

[Challenges](#_bpo7i8je814y) 8

[Risk Assessment](#_lbrhm2se7fa1) 9

[**CHAPTER 4**](#_63wlrs9f19j1) **10**

[CONTINGENCY PLAN](#_mrm598xurvta) 10

[Baseline Security Requirements](#_j98t9uz9uslt) 10

[Handling Security Incidents](#_j98t9uz9uslt) 10

[National awareness exercises](#_ccbmt89sis4i) 11

[Information Exchange Mechanism](#_j98t9uz9uslt) 11

[Support for R&D](#_j98t9uz9uslt) 11

[Cooperation at International Level](#_j98t9uz9uslt) 12

[**REFERENCES**](#_eb15qrgmvmwt) **13**

# 

# 

# EXECUTIVE SUMMARY

With the rapid development in the field of Information and Communication technology(ICT), Cyber Security Strategy has become a necessity for Cyberia. Cyberspace has now become a platform for growth, innovation, prosperity and development. Cyberia has always focused on providing a secure and risk free cyberspace for the citizens however all the threats can not be mitigated. Thus to address seen as well as unseen threats in cyberspace, a comprehensive national cyber security strategy is essential.

To create the cyber security strategy, initial analysis of the cyberspace was performed. First chapter focuses on providing an overview of Cyberia. The overview provided a guideline on how the cyber security strategy must be prepared. Infrastructures were identified, government bodies were listed and existing policies were studied. Initial objectives were prepared based on the overview of Cyberia.

Second chapter focused on the vision of the cyber security strategy and initiatives taken in Cyberia. Based on the objectives defined in this chapter, further sub-objectives were created and strategies were prepared on that basis.

Third Chapter solely focuses on why cyber security strategy was needed for Cyberia. Prior to creating the strategy, initial threat analysis and risk assessment were performed. The result then led to creation of strategies and policies. Based on the identified threats and foreseen challenges, risk assessment was performed, critical infrastructures were then identified.

After identifying the critical infrastructures, it was now time to create strategies to cover those areas. The strategies were created defining line of action, scope and detailed plan. The overall contingency plan included six main areas with critical infrastructure in it, basic security requirements, handling security incidents, national awareness exercises,support for resource and development and cooperation at international level.

Fifth and last Chapter includes what will be the plan moving forward. Policies will be created based on the existing strategy. The policy will focus on further development of ICT in Cyberia.

# CHAPTER 1

## OVERVIEW OF CYBERIA

**Geography and Infrastructure:** Southern European country - Cyberia. Average size (10m inhabitants) with a harbor and a coast of ¼ countries borders length. Also includes airports, railways, and roads.

**Political system and Public Relations:** Democratic country, that re-elects their Prime Minister and President every four years. No internal conflicts, nor international conflicts. Some unstability around in the neighboring countries. NATO base close by. Member of European Union, but not the eurozone. Relationships with Interpol.

**Military and Internal Affairs:** Cyberia’s military consists of around 15,000 soldiers if needed. Corruption was part of the culture, but has decreased drastically for the last 4 years.

**Public Safety and Assurances:** Free Healthcare, digital journal is being tested and evaluated in order to continue its development. The government assures officers such as: customs, border police, coast guard. Cyberia has a civil contingency agency.

**Internet Infrastructure:** No internet censorship, 3 different ISP for public use, two internet exchange points, 3G is well spread, 4G is in the process, covers the capital city. Most people use ADSL connection to the internet, while capital city populace can enjoy fiber, but only the wealthy.

**Education:** Mostly everybody has earned at least a highschool diploma, often continues studies at national universities or goes to study abroad.

**Natural and Human-Created Resources:** Aluminum, Steel, Coal. Power supply is managed by nuclear power plants, coal, and some wind power.

**Threats**: Super Power nation nearby. Gun and drug smuggling. High unemployment

**Other Facts:** Refugees from North Africa and the Middle East. Peaceful state, but can change due to political reasons and conflicts.

# CHAPTER 2

## LINE OF ACTION DEFINITION

### Vision

The national cybersecurity strategy of Cyberia will be established on the basis of secure and responsible networks, systems and use of information by enhancing and developing its capabilities to prevent, detect and respond to the evolving cyber threats. At the same time, specific measures should be followed and implemented in order to provide a secure cyberspace to the society. As a result, an effective NCS will ensure a resilient cyberspace, the protection of citizens’ rights, the transparency in society and at the same time, it will enhance the national security and socio-economic progress. The cyber vision of Cyberia for 2020 is :

***A secure, resilient and trusted nation promoting socio-economic development and threat free cyber space.***

### Objectives

The Cyberia’s strategy should implement the following objectives:

* Enhanced security and resilience on the available information, networks and systems for businesses, public sector and essential services.
* Ensure the reliability and security of cyberspace in order to tackle cybercrime and malicious use in general.
* Ensuring the protection of citizens, society and businesses in an open and vibrant cyberspace.
* Improving human knowledge, skills and capabilities with the aim to build a cybersecurity culture in the society.
* Promote an international cyberspace strategy.

### Initiative

The NCS of Cyberia will be based on the following initiatives:

* Creating a NCS in compliance with the national security strategy, EU’s initiatives (such as CSDP, GDPR) and other international normes.
* Implement a public body/agency as a coordinator of the NCS where roles, responsibilities and accountability of all stakeholders are well defined (ref. enisa).
* Joint-effort and enhanced collaboration between state,businesses and citizens will be promoted as it will strengthen cyber and information security in several societal and business aspects.
* Improve and monitor communication networks, systems and credibility of information with regard to central government and related critical infrastructures.
* Enhance the cybersecurity awareness of citizens, governmental bodies and businesses through specific development campaigns.
* Promote the international cooperation with regard to cyber security through presence in multinational organizations.
* Reinforce and improve national defensive systems in order to tackle future cyber threats.

# CHAPTER 3

## NEED FOR CYBER SECURITY STRATEGY

**Threats challenged Cyberia for Cyber Security Strategy!**

Cyberspace is full of opportunities for both good and bad. The vast and easily accessible cyberspace amplifies the threats of the cyber world. The existence of threats and challenges in ICT created the necessity for cyber security strategy. Based on the threats and challenges, multiple risk levels and critical infrastructures were identified.

### Identification of Critical Infrastructure

* The Defense Industrial Base Sector
* The Information Technology Sector
* The Nuclear Reactors, Materials, Waste and Energy Sector
* The Financial Services Sector
* The Government Facilities Sector
* The Food and Agriculture Sector
* The Water and Wastewater Systems Sector
* The Healthcare and Public Health Sector
* The Emergency Services Sector
* The Education Sector
* The Chemical Sector
* The ISP and Communications Sector
* The Critical Manufacturing Sector
* The Commercial Facilities Sector
* Transportation System Sector

### Threats

Cyberia identified following to be main threats to the cyberspace nationwide:

|  |  |
| --- | --- |
| **Threats** | **Descriptions** |
| Advanced Persistent Threats | Attacks to achieve specific malicious goals by gaining unauthorized access for the purpose of continuous attack over a long period of time (What is an Advanced Persistent Threat (APT)?, 2020). |
| Phishing | Cyber attack performed by using disguised email as a choice of weapon (Fruhlinger,2020). |
| Hacking | Activities performed to compromise digital devices (What is Hacking - Everything You Need to know, 2020). |
| Data Leakage | Phenomenon where data is transmitted from an organization/country to an external entity (What is Data Leakage?, 2020). |
| Cyber Crime Syndicates | Group of people working together to perform cyber crimes. |

### Challenges

The following challenges were identified with regard Cyberia’s NCS:

* Achieve a sufficient level of cyber resilience in a national level with regard to the evolving cyber threats.
* Build and execute a comprehensive cybersecurity strategy which will address Cyberia’s and global cybersecurity needs.
* Be able to secure Cyberia’s critical infrastructures and sensitive information from a malicious cyber attack to ensure the prosperity of society.
* Take the appropriate countermeasures and use effective preventive systems in order to enhance the response and recovery from malicious incidents.
* Promote the cooperation between government, businesses and citizens with regard to cybersecurity and at the same time, increase the level of cyber security awareness.

### Risk Assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat** | **Vulnerability** | **Asset** | **Impact** | **Likelihood** | **Risk** |
| Network Failure | ISP providers are limited (4) | Website | All web services | Other standby service provider able to assist within specific time range | Potential loss of $1324973495 per hour |
| Server Failure | Power dependent on 1 nuclear plant | Data centers, Servers, Desktop, Laptops | All power operated devices | Last downtime in nuclear plant occured 4 years ago which lasted 15 minutes | Potential loss of $2497943 per hour |
| Human errors | Citizens are moderately educated | Data | Data within range of accidental human error | Likelihood high because of lack of cyber strategy | Not applicable |
| Malicious attacks | Crime exists, might transpose to cyberspace | Public and Private websites of Cyberia | Website might be unavailable | DDOS attacks are discovered every 6 months | Potential loss of $18000 per hour |

# 

# CHAPTER 4

## CONTINGENCY PLAN

### Baseline Security Requirements

Majority of Cyberia’s ICT includes digital devices which are individual and non-government organizations owned. Many do not realise the risk that comes with the use of technologies, these fields have always been targets for cyber threats. Even those who are well educated to recognize the risk of cyber threats are having difficulty identifying affordable and effective measures to protect themself from the imposed risks. Cyberia will be taking a leadership role in cyber security to help organizations and its citizens to recognize the values of cyber security and support efforts to maximise the baseline of cyber security. Cyberia will determine the minimal security requirements based on the risk assessment, which organizations and individuals must implement to achieve the fundamental baseline security requirements. This indeed will be beneficial in reducing the threats that cybercriminals possess in Cyberia.

### Handling Security Incidents

Cyberia will create a new body ‘National Security Implementation Center’ or (NSIC) by the end of 2020 for better support of security of government ICT and critical infrastructures. Specialist team will be formed within NSIC which will include but not limited to Threat Intelligence, Incident Response, Awareness Training and Network Monitoring. The unit will continue to function as the point of contact for nationwide cyber security incidents and will proceed to lead the response to those incidents at all levels.

### 

### National awareness exercises

Increasing cyber security awareness is an essential element of an effective NCS . As a result, Cyberia’s government will promote awareness training programmes that will target businesses, citizens and governmental institutions and they will be tailored with regard to the specific target group and training level. In addition, the programmes will be divided regarding the business size in order to achieve better results. At the same time, training programmes will be organized in schools and universities, tailored for different educational levels and specialities, as we strongly believe that cybersecurity awareness should be promoted from early ages. Furthermore, Cyberia’s state should promote university programmes which will be specialized in information security in order to create a sufficient number of skilled experts. (enisa + spanish NCS)

### Information Exchange Mechanism

Every citizen of Cyberia will have a right to free cyberspace. Any personal data collection will take place in compliance with General Data Protection Regulation. Information Sharing Systems will be present in the country and information like: home address, phone number, car registered to peoples names, any previous or ongoing criminal activities, known debts, will be collected. This information will not be accessible to the public unless it is related to criminal activities according to the law of Cyberia or EU. To further, Cyberia will cooperate with Interpol, NATO and European Union States to reach maximum integrity in the country and a better future world for all.

### Support for R&D

Cyberia will enhance and support a transparent, safe and innovative cyber world, therefore will continue its pursuit for partnerships and creation of national programmes in schools, higher education institutions, industrial research institutes and other private and public sector entities. The main focus will be to find new threats, analyze them and create solutions. To further, it will create positions for young cyber security specialists and scholarship opportunities to pursue careers within the cyber security field to initiate new research and development ideas in order to produce a safe and innovative environment online.

### Cooperation at International Level

Cyber security and the threats evolving in the domain have a global nature (enisa). Cyberia’s NCS will promote international cooperation in a bilateral and multilateral level by taking an active presence in multinational organizations such as EU, NATO and UN with regard to the development of a secure cyberspace, knowledge and information sharing. In addition, the coordinator of this action will be the public body that will be developed with specialization in cybersecurity in order to achieve a consolidated presence. Furthermore, Cyberia should join conventions and treaties related to information security in a bilateral or multilateral level that comply with the national security strategy. To conclude, Cyberia will seek to play a critical role in the cooperation of the EU and NATO as a member state.

## 

# REFERENCES

Forcepoint. 2020. *What Is An Advanced Persistent Threat (APT)?*. [online] Available at: <https://www.forcepoint.com/cyber-edu/advanced-persistent-threat-apt> [Accessed 7 May 2020].

Fruhlinger, J., 2020. *What Is Phishing? How This Cyber Attack Works And How To Prevent It*. [online] CSO Online. Available at: <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html> [Accessed 7 May 2020].

Malwarebytes. 2020. *What Is Hacking - Everything You Need To Know*. [online] Available at: <https://www.malwarebytes.com/hacker/> [Accessed 7 May 2020].

Forcepoint. 2020. *What Is Data Leakage?*. [online] Available at: <https://www.forcepoint.com/cyber-edu/data-leakage> [Accessed 7 May 2020].