HELLENIC REPUBLIC
MINISTRY OF DIGITAL GOVERNANCE
NATIONAL CYBERSECURITY AUTHORITY

NATIONAL CYBERSECURITY STRATEGY 2020 - 2025


NATIONAL
CYBERSECURITY
AUTHORITY


National Cyber Security Authority
HELLENIC REPUBLIC

NATIONAL CYBERSECURITY STRATEGY 2020 -2025

DECEMBER 2020

ABBREVIATIONS GLOSSARY

OES	Operator of Essential Services
DSP	Digital Service Provider
CERT or CSIRT	Computer Emergency Response Team or Computer Security Incident Response Team
SLA	Service Level Agreement
SOC	Security Operations Center
SIEM	Security Information & Event Management
SOAR	Security Orchestration and Response
MDR	Managed Detection and Response
ICT	Information and Communication Technology/ies
Entities	A term that includes the bodies of the wider Public Administration, the OES (Operators of Essential Services), the DSP (Digital Service Providers) and in general, organizations which are subject to the provisions of Law 4577/2018
GSTP	General Secretariat of Telecommunications and Post
MSSP	Managed Security Service Provider
CISO	Chief Information Security Officer

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

Continuous adaptability, prevention, and timely response to challenges in a changing environment consist the firmest foundation for the effective development of an integrated strategy to address cyber-attacks. Since 2018 and the 3rd revision of the National Cybersecurity Strategy, important technological developments (e.g. 5th generation mobile networks, artificial intelligence, IoT) have occurred. What is more, the rapid spread of an unprecedented pandemic (COVID - 19) with shocking consequences for humanity, triggered the need for increased use of new technologies and digital applications to serve citizens and businesses. All these developments necessitate the immediate evaluation and feedback of the cyber security strategic planning in Greece. As a matter of fact, the more society and economy rely on the digitization of procedures and services, the greater the attack surface becomes (that is the range of opportunities for malicious actions), calling on timely planning and effective response from all stakeholders.

Our country, participating in all relevant European and international fora and acknowledging the fundamental importance of security shielding of information and communication systems and networks, has already taken several important initiatives aimed at meeting international and EU requirements, creating a secure environment for new technologies and increasing the confidence of citizens and businesses in digital applications and services for the benefit of the economy and society. These initiatives include: the entry into force of Law 4577/2018 “Transposition into Greek legislation of the Directive EU 2016/1148 of the European Parliament and of the Council on measures for a high common level of security of network and information systems throughout the Union and other provisions ”(A’ 199) and the issuance of the ministerial decision 1027/2019 (A’ 3739) on the basis of which the framework of obligations for the OES (Operators of Essential Services) and the DSPs (Digital Service Providers) was determined, including the security requirements they must comply with, the upgrade of the National Cybersecurity Authority to a General Directorate of the Ministry of Digital Governance, the planning and participation of the competent services in preparedness exercises, the use of advanced systems for preventing and dealing with cyber-attacks, etc.

Within this context, and considering the latest requirements and needs, the National Cyber Security Authority of the Ministry of Digital Governance, being the competent authority in accordance with the provisions of L. 4577/2018 and p.d. 40/2020 (A ‘85), hereby proceeds to the national cybersecurity strategic plan update, as to perform an in depth assessment of the current situation, identify new challenges and develop an appropriate strategic framework for immediate implementation.

2 SITUATION ANALYSIS

2.1 A RAPIDLY CHANGING CYBER THREATS ENVIRONMENT

The European Union's Member States may be considered as potential targets for numerous cyberattacks, as a result of technological progress, developments in digital governance, as well as their achieved level of prosperity. The cyber-threat environment, either it involves threats from individual criminals or alleged state-sponsored attacks, is rapidly changing, leading to an inherent inability to provide immediate protection. These conditions confirm the need for a periodically updated strategy, which will set the rules for addressing or mitigating the impact of these threats.

In the European Union, various attacks have been recorded, aiming at different targets, as shown in the figure below, provided by the ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	▶	1. Malware	▶	▶
2. Web Bassed Attacks	▲	2. Web Bassed Attacks	▲	▶
3. Web Application Attacks	▲	3. Web Application Attacks	▶	▶
4. Phishing	▲	4. Phishing	▲	▶
5. Spam	▲	5. Denail of Service	▲	▲
6. Denial of Service	▲	6. Spam	▶	▼
7. Ransomware	▲	7. Botnets	▲	▲
8. Botnets	▲	8. Data Breaches	▲	▲
9. Insider threat	▶	9. Insider threat	▼	▶
10. Physical manipulation/ damage/theft/loss	▶	10. Physical manipulation/ damage/theft/loss	▶	▶
11. Data Breaches	▲	11. Information Leakage	▲	▲
12. Identity Theft	▲	12. Identity Theft	▲	▶
13. Information Leakage	▲	13. Cryptojacking	▲	NEW
14. Exploit Kits	▼	14. Ransomware	▼	▼
15. Cyber Espionage	▲	15. Cyber Espionage	▼	▶

Legend: Trends: ▼ Declining ▶ Stable ▲ Increasing - Ranking: ▲ Going up ▶ Same ▼ Going down

Figure 1 *ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends*

According to the latest ENISA data (ETL 2020, List of top 15 threats, enisa.europa.eu):

- Phishing attacks have already risen to 3rd place, while web application attacks have fallen to 4th place,
- Spam attacks rose to 5th place and DDoS attacks dropped to 6th place
- Identity theft attacks rose from 13th to 7th place
- The case of botnets is now in 10th place
- The case of physical manipulation, damage, theft and loss dropped to 11thposition
- Similarly the information leakage cases dropped to 12th place
- Ransomware rose to 13th place
- Cyberespionage cases rose to 14th place
- Crypto-jacking cases are in 15th place

TOP 15 CYBER THREATS

1 Malware	2 Web Bassed Attacks	3 Phishing	4 Web Application Attacks	5 Spam
6 DDoS	7 Identity Theft	8 Data Breache	9 Insider threat	10 Botnets
11 Physical manipulation/ damage/theft/loss	12 Information Leakage	13 Ransomware	14 Cyberespionage	15 Cryptojacking

Figure 2 *ENISA, ETL 2020 (enisa.europa.eu), Top 15 Threats*

In more detail, the threats have as follows:

2.1.1 Malicious Software

Software specifically designed to cause damage or gain unauthorized access to a computer system. It attacks a computer or network in the form of viruses, worms, trojan horses, etc. Ransomware also belongs to this category, but it is examined separately due to its special nature.

2.1.2 Web based attacks

This involves threats that target the user directly by exploiting browser vulnerabilities, as well as content management systems. Main types of attacks in this category are browser exploits, drive-by downloads, watering hole attacks etc.

2.1.3 Phishing

It refers to malicious e-mails or telephone conversations which intend to mislead users and reveal confidential information.

2.1.4 Web application attacks

This case involves attacks targeting web applications. These applications due to their universal use in content delivery are the target of multiple types of attacks, such as cross-site scripting (XSS), SQL injection, path traversal, local file inclusion etc.

2.1.5 Unwanted e-mail messages

Also referred to as SPAM, these attacks involve sending spam to users. This correspondence is characterized by the very low cost of sending messages, the inconvenience it causes to users, but also the potential transformation of messages into phishing threats.

2.1.6 Denial of Service (DoS attacks)

It refers to attacks in which a large volume of internet traffic targets a service, to make it impossible for the systems to serve legitimate requests. Essentially, they take advantage of the finite capacity of systems and networks to make it impossible to provide services (loss of availability).

2.1.7 Identity theft

The attacker obtains personal data of the user (passwords, social security numbers, etc.), resulting in the appropriation of the user's identity (impersonation) and for the purpose of financial gain (product purchases with credit cards, illegal tax refund, etc.) to his/her detriment.

2.1.8 Personal data breaches

This involves attacks aiming to the leakage, alteration, or unavailability of personal data. According to the EU Regulation 2016/679, such attacks are regarded as breaches of personal data which need to be addressed immediately.

2.1.9 Insider threat

It refers to threats arising from organizations' employees, as well as external contractors who hold internal information about the organization's security practices, computer systems and data. These threats can lead to several attacks described in this section, usually with a vast impact on an Agency and are extremely difficult to diagnose and / or tackle.

2.1.10 Botnets

It involves networks that consist of malicious computer devices infected with malware and are centrally controlled by an attacker to be used as a group to send spam, denial of service attacks, crypto jacking, etc.

2.1.11 Natural threats

It refers to threats aimed at destroying, altering, or stealing equipment, with the goal of leaking and / or destroying data or denying service.

2.1.12 Data leakage

It involves data leakage to unauthorized users. The data may include financial data, patents, copyrighted data, strategic development plans, etc.

2.1.13 Ransomware

It is malware that encrypts information system data, for the encryption of which the attacker requires ransom (usually in the form of cryptocurrency).

2.1.14 Electronic espionage

Cyber espionage, which may involve the use of specialized tools to extract information and / or use a combination of the aforementioned threats. Usually, this form of attack is referred to as "targeted" (because the attackers have very specific goals). Their goal is to intercept sensitive information.

2.1.15 Crypto jacking

It refers to techniques that use the computing power of the user's computer to extract (mining) cryptocurrencies (bitcoins).

2.2 THREAT AGENTS

The main threat agents are summarized in the following categories. Their general rating is provided regarding the level of difficulty in recognizing the attacks, their impact, and the probability of their occurrence[1].

2.2.1 Cybercriminals

Cybercrime, as a term, is broadly used to describe any criminal activity that is intended to have an impact on the operations of an organization using ICT technologies. Consequently, cybercriminals, as threat agents, are groups or individuals who use technology (ICT) to commit malicious criminal acts[2]. These agents are often involved in illegal transactions on the so-called Dark Web, where they buy and sell malware or information for potential targets.

Cybercrime, in the context of this Strategy, may include:

- Terrorist acts (cyber-terrorism)
- Denial of Service (DoS - cyber extortion) attacks
- Cyber warfare

A special category is considered to be the so-called script kiddies, who use tools developed by third parties and / or other threat agents (e.g. hackers) seeking fame through their act or the acquisition of small amounts of money in exchange for non-disclosure of personal data (e.g. personal photos) or systems decryption (if they have been infected with malware such as ransomware). Although they may affect the continuity of operations, the difference with the rest lies in the unorganized nature of their attacks and / or the non-targeting of entities.

2.2.2 State - sponsored attacks

This factor includes groups that either belong to or are funded by states. These groups are primarily aimed at launching attacks that will have a major impact on the provision of basic / essential services by entities. The main purpose of such attacks is to interrupt services (e.g. through denial of service attacks - DoS / DDoS) or unauthorized access to classified data. Special mention should be made of cyber-espionage cases, where in recent years[3], an escalation of attacks on OES may be observed.

Attacks in this category are usually characterized by their persistence and the fact that they have been designed in detail to deliver critical hits.

It is customary for cyber groups to attack Public Administration bodies or OES / DSP in the name of a third state. However, these attacks, which are mainly aimed at altering the content of websites and / or temporarily denying services, must be taken seriously in the context of activism, and not as a result of actions sponsored by third countries.

It involves self-proclaimed activists or similar groups that carry out malicious actions such as denial of service attacks, website hacking,

[1] The general classification is based on research in the field of cybersecurity (e.g. ENISA and other bodies)

[2] Within the context of the Cyber Security Strategy, cyber-attacks are examined rather than the malicious actions by organized crime which can use ICT to increase its impact (e.g. carnage). Consequently, the Strategy focuses on tackling "cyber-dependent crimes" rather than "cyber-enabled" (HM Government, National Cyber Security Strategy 2016-2021, UK)

[3] ENISA Threat Landscape Report, 2008

attacks / counterattacks on states, etc. The goal of activists (often referred to as hacktivists) is to promote a social change or political agenda or a counterattack aiming at nationalism stimulation \, which is often accompanied by a warning to cease the “operative cause” under the threat of prolonging and / or repeating and / or escalating the attack.

2.2.3 Activists

This factor applies to employees of organizations that carry out, either intentionally or unintentionally, malicious acts. Due to the nature and level of access to systems and information of an entity, as well as the perimeter security approach adopted by several agencies, internal threats are one of the most serious threat factors, as well as one of the most difficult to identify and address.

2.2.4 Internal threats

2.3 NEW CHALLENGES ARISING FROM CONTEMPORARY TECHNOLOGIES - (5G NETWORKS, ARTIFICIAL INTELLIGENCE, BIG DATA, CLOUD COMPUTING, IoT)

Technological developments are accelerating globally, entering a new trajectory of application design and networking services. In the context of the new 5th generation network technology, where the connectivity speeds are estimated to reach up to 20 Gigabits per second[4], optimization of new technologies utilization, ranging from the household unit (smart home) and the level of business (smart business) to the level of cities (the so-called smart cities) can be achieved. As a matter of fact, this could also be stated for entire service sectors.

New technologies, such as artificial intelligence, the ability to further develop smart machines and devices (smart phones, smart cars, smart devices), combined with cloud computing technologies and the new networking capabilities of 5th generation networks, provide a wide range of applications in the field of health (Internet of Medical Things - IoMT, digital health system, interconnection of health services and health resources), transport (at the level of vehicle, driver, and infrastructure, resulting in innovative services in the field of road security, travel, logistics, etc.), the construction sector (Industry 4.0), the agri-food sector, but also other sectors such as national defense (Internet of Military Things). Consequently, it is no coincidence that we are already talking about the Internet of Everything (IoE).

Along with these developments, the COVID-19 pandemic has set new standards and demands across the spectrum of economic and social life. The challenges and difficulties arising from the personal contact restrictions among people due to the increased risks of transmitting the disease, the restrictive measures taken worldwide, the closure of shops and public gathering places, are all issues looking for alternatives in the digital world: teleconferencing (teleconference, telco), video calls, remote access, e-shops, the “digital state”.

However, these developments, combined with the growing demand for digital applications and services, pose significant challenges. The faster the expansion of the digital world to every aspect of daily economic and social life, the wider the surface for malicious and illegal activities. The more contemporary digital services are getting personalized and targeted to our needs, the greater the risks of exploiting or violating our personal data. The handier it is for us to communicate with friends and associates around the world using ICT technologies, the easier it can be for malicious actors to make use of our exposure to social networking sites as to perform illegal activities. These are just a few examples of the fact that not only technology by itself, but especially the way we use it, carries various risks. For these reasons, the development and implementation of a holistic cybersecurity strategy should focus not only on the constant influx of knowledge, the understanding of modern technological developments and the provision of specific safeguards, but also on the constant information and awareness of users in the context of the promotion of cyber-hygiene.

[4] See IMT-2020 (ITU) https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Documents/S01-1_Requirements for IMT-2020_Rev.pdf

2.4 THE 2018 NATIONAL CYBERSECURITY STRATEGY. PRIORITIES AND EVALUATION

In March 2018, following a proposal by the National Cyber Security Authority, the 3rd Revision of the National Cybersecurity Strategy was issued (Online Publication Number: Ψ4P7465XΘ0-Z6Ω). The strategy was aligned with the following general principles:

- The development and consolidation of a secure and resilient cyberspace
- The continuous improvement of our capabilities in defending cyber-attacks with an emphasis on the protection of critical infrastructures, as well as safeguarding operational continuity
- The formulation of the national cybersecurity framework, to ensure effective response to cyber-attacks and minimize the impact of cyber threats
- The development of strong cybersecurity culture across the public and private sector, as well as the citizens, utilizing the relevant involvement of the academic community as well as the public and private entities

In addition, the National Authority developed a strategic plan based on a total of thirteen (13) objectives outlined as follows:

Identifying stakeholders to be involved in the National Cybersecurity Strategy. Stakeholder mapping.

Identifying critical infrastructure

Assessing risks at national level

Mapping and improving the existing institutional framework

Developing a national contingency plan in the cyberspace

Establishing security baselines

Addressing Security Incidents

Performing national cybersecurity exercises

Promoting users'-citizens' awareness

Establishing reliable information sharing mechanisms

Supporting the implementation of R&D and academic educational programs

Cooperating at international level

Evaluating the National Cybersecurity Strategy

Figure 3
The 13 objectives of the 3rd Review of the National Cybersecurity Strategy (2018)

As regards the development and goal - setting of the current strategic cyber security planning, our country follows European standards and methodologies. Within the context of the evaluation of this strategic framework, the National Cybersecurity Authority utilized the application of an evaluation tool (national cybersecurity strategies evaluation tool), created by the European Cybersecurity Organization (ENISA) which includes a total of fifteen (15) objectives.

Develop national cyber contingency plans

Protect critical information infrastructure

Organize cyber security exercises

Establish baseline security measures

Establish incident reporting mechanisms

Raise user awareness

Foster R&D

Strengthen training and educational programs

Establish an incident response capability

Address cyber crime

Engage in international cooperation

Establish a public – private partnership (PPPS)

Balance security with privacy

Institutionalize cooperation between public agencies

Provide incentives for the private sector to invest in security measures

Figure 4
The fifteen (15) objectives for evaluating national cybersecurity strategies, ENISA (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool)

Considering the conclusions of the gap analysis, conducted by the National Cybersecurity Authority, the areas of strategic emphasis for the current, 4th Review, can be summarized into six (6) priorities: Contingency Planning, Incident Reporting, Security and Privacy protection, Research and Development, Public-Private Partnerships (PPPs), Investments in security measures. In more detail, for each of the above, special areas of emphasis are analyzed in the table below:

Strategy priorities	
Contingency planning	• National crisis management planning • Regular updates and reviews of the contingency planning • Sharing information • Development of risk management capacity (identification, analysis and risk impact assessment, vulnerability assessment) • Cyber threat reports • Use of platforms • Establishment of a national risk register • Tools and platforms for situation awareness
Incident reporting	• Coordination under the NISD, GDPR, Article 13A and eIDAS • Best practices for compiling annual incident reports at national level • Sectoral incident reporting plans and field reports
Security and Privacy Protection	• Coordination with personal data security framework • Training and awareness raising
Research and Development (R&D)	• Setting priorities • Mechanisms for development and diffusion of innovation (e.g. startups, clusters, etc.) • R&D financing
Public-Private Partnerships (PPSs)	• National framework • Funding and incentives
Investment in Security Measures	• Best practices • Support for startups and SMEs • Procedures

Figure 5
Areas of emphasis to be included in the strategic review

3 GUIDING PRINCIPLES AND VISION OF THE NATIONAL CYBERSECURITY STRATEGY 2020 -2025

3.1 GUIDING PRINCIPLES

Under the current framework, the basic principles for the protection of entities -and key pillars for strategic formulation- are being defined as follows:

- All actions outlined in the Strategy and the Action Plan aim at the protection of citizens and entities, constituting the basis which the digital governance and prosperity of the country rely on.

- All cyber threats and factors that may affect the operational continuity of the Public Administration and other stakeholders are identified, recorded, categorized, and treated with due diligence.

- The protection of human life and human rights (such as the protection of personal data in particular) is of the utmost importance for the Strategy. The National Cybersecurity Authority and the entities shall take all possible measures to ensure the protection of citizens in accordance with the applicable laws and regulations.

- The successful implementation of the Strategy requires collective effort and partnership between stakeholders. Consequently, cooperation between private and public entities, the strengthening of research and development in the cybersecurity domain, as well as the information sharing between national and European Agencies, with a view to the continuous optimization of the Strategy and its implementation measures, are being emphasized.

- The effectiveness of the Strategy in ensuring the continuity of the entities' operational activities, is based on the constant information and education of all entities involved, as well as the citizens.

- The Strategy sets the framework for defining specific objectives, roles, and responsibilities, as well as indicators that will assist in its ongoing evaluation and review, in line with the changing ICT environment and threats, but also the services requested by citizens.

3.2 VISION STATEMENT

In light of the above principles and priorities, the vision statement of the new National Cybersecurity Strategy has as follows:

"A modern and secure digital environment of information and network infrastructures, applications and services for the benefit of economic and social prosperity, aimed at guaranteeing the protection of citizens' fundamental rights, developing a culture of secure use of digital services and applications, as well as increasing citizens' and businesses' confidence in digital technologies."

KEY ELEMENTS OF THE VISION ARE:

- Building a modern digital environment: building a digital environment that allows the continuous inflow and development of new technologies and innovations in the digital age.

- Establishing a high level of cyber security: cyber security across the range of information infrastructures, applications, and services, adapted to the ever-changing challenges and requirements.

- Ensuring the protection of fundamental rights: in particular, the protection of personal data, the protection of privacy, the free development of personality, equality, and participation in the digital society.

- Developing a culture of safe use: safe use in the sense of digital education, continuous information and awareness of the risks and pitfalls of new technologies.

- Increasing confidence in digital governance: the key achievement of a secure digital environment, i.e., the use of new technologies across the spectrum of social and economic life for the benefit of citizens, businesses, and socio-economic prosperity.

4 METHODOLOGY

4.1 FIVE (5) STRATEGIC OBJECTIVES

First and foremost, the results of the analysis of strategic priorities are utilized to formulate a total of five (5) emblematic objectives for the development of strategic planning, covering all fifteen (15) specific strategic development objectives provided by ENISA for the EU Member States, as follows:

Figure 6
Defining strategic goals based on strategic priorities

Strategic Goals	Achieved ENISA Objectives for EU Members
1. A functional cybersecurity governance system [5]	**1.A.** Optimize organisational structures and procedures
	1.B. Apply vigorous risk assessment and effective contingency planning
	1.C. Strengthen national, European, and international collaborations
2. Shielding Critical Infrastructures and securing new technologies	**2.A.** Comprehend technological developments and their effects on digital governance
	2.B. Upgrade critical infrastructures' protection
	2.C. Consolidate systems and applications by implementing enhanced security requirements
3. Incident management optimisation, fight against cybercrime and privacy protection	**3.A.** Optimise methods, techniques and tools utilised in incident analysis, response and reporting
	3.B. Strengthen deterrence mechanisms and enhance operational cooperation
	3.C. Cybersecurity for the protection of privacy
4. A modern environment for cybersecurity investments with emphasis on the promotion of Research and Development	**4.A.** Encourage R&D initiatives
	4.B. Provide investment incentives
	4.C. Utilise PPPs
5. Capacity building, promoting information and awareness raising	**5.A.** Building capacity by organising cybersecurity excersising activities
	5.B. Apply state - of - the - art educational and training methods and tools
	5.C. Promote open - ended cybersecurity information and awareness raising for Entities and citizens

[5] It is noted that any reference to a governance system, within the present document, concerns the cyber security governance system

Figure 7
Five strategic goals for the development of strategic planning

For each of the above strategic goals, specific objectives are being developed aiming at the specialization and better management of the strategic framework (cascade effect). These objectives are further specified into activities that cover the full range of recognizing, preventing and protecting, deterring and recovering from cyberattacks.

4.2 FIFTEEN (15) SPECIFIC OBJECTIVES

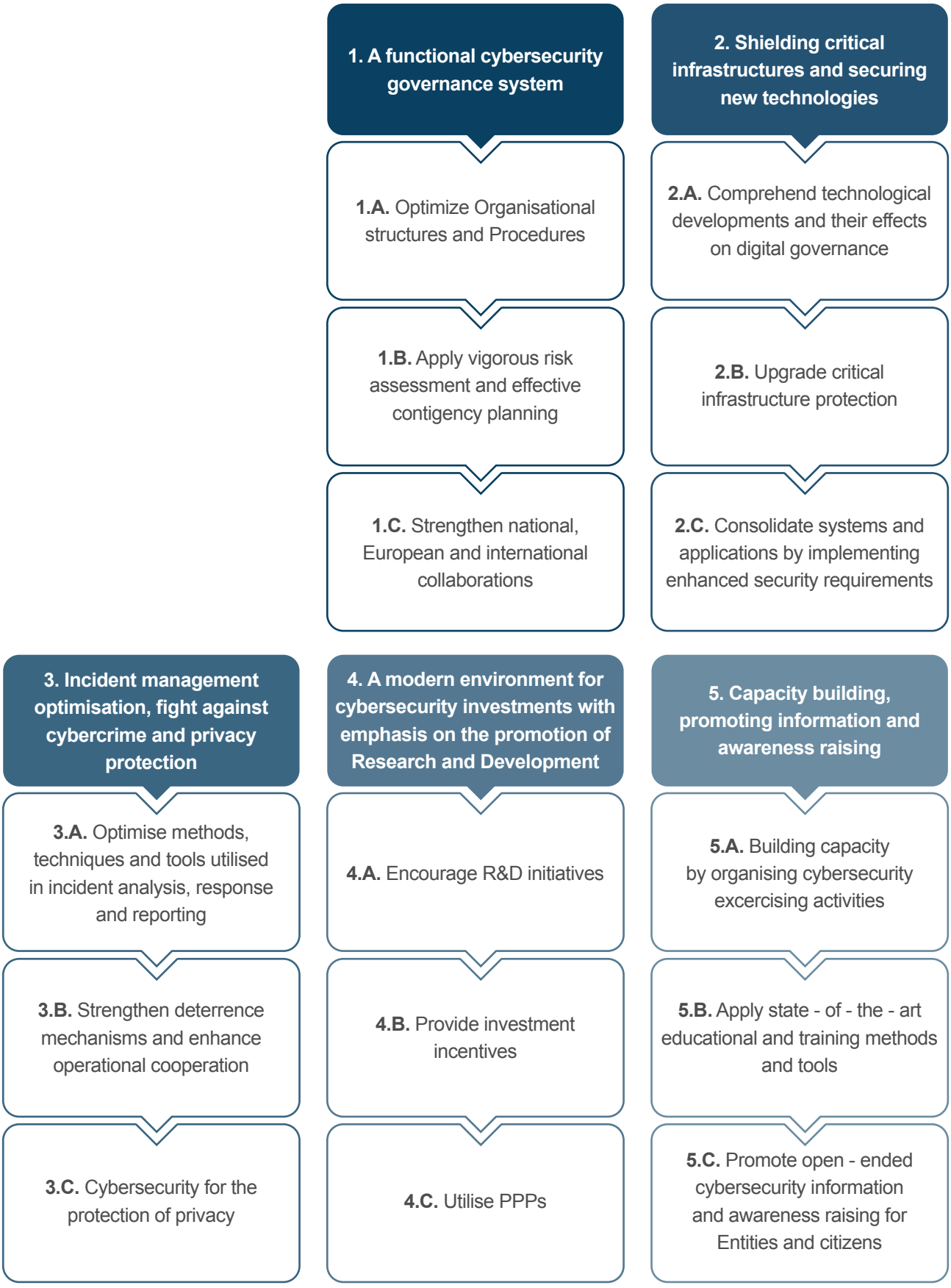

Figure 8 *Goal – setting framework of the National Cybersecurity Strategy 2020-2025*

5 STAKEHOLDER MAPPING

Performing a stakeholder mapping is deemed as an essential goal, in the context of the 3rd Revision of the National Cybersecurity Strategy. A detailed reference to the stakeholders, whose coordination and involvement in all stages of the national strategy implementation emerges as a critical success factor, is provided below.

5.1 DIRECTORATE - GENERAL FOR CYBERSECURITY – NATIONAL CYBERSECURITY AUTHORITY

The Directorate – General for Cyber Security of the Ministry of Digital Governance (National Cyber Security Authority- NCSA), is responsible for managing the implementation of the Cybersecurity Strategy and the coordination of entitiess throughout the enactment of the required measures. Over the implementation of the Strategic Plan, the NCSA aims at the definition of appropriate organisational, technical and operational measures and their implementation by the respective entities, the evaluation of the Strategy, and its revision. In particular, the responsibilities of the Authority include, inter alia, the following:

- Overall management of the National Cyber Security Strategy
- Identification of baseline security requirements
- Regulatory framework drafting and implementation management
- Collection and registration of security policies
- Collection and assessment of OES recovery plans
- Assessment of security policies and procedures to prevent and counter security incidents
- Identification, updating and evaluation of services and functions that are based on or affect information security (e.g.cloud services, security strategy and guidelines for mobile telephony, new mail applications), Research and development support
- Implementation of a cybersecurity and incident management framework
- Audit and evaluation of entities

- Critical infrastructure monitoring
- Application of technical security checks (e.g. penetration tests), carrying out training programs, technical trainings for administrators and cybersecurity exercises, as well as keeping CISOs updated on possible threats
- Issuance of Standards and circulars
- Issuance of basic security architecture principles
- Recording of the Strategy's KRI/KPI effective implementation indicators of each entity
- Response to security incidents affecting the NCSA and / or other entities and coordination of actions
- Incident log management
- Crisis management and National Emergency Plan activation
- Basic security requirements evaluation and review
- KPI / KRI metrics and National Emergency Plan evaluation and review
- Supervision and coordination of entities' CISOs
- CISOs registry management
- Cooperation, on cybersecurity issues, with national authorities (e.g. Hellenic Data Protection Authority, Hellenic Authority for Communication Security and Privacy etc.) and the academia
- European and international level cooperation, representation and communication management (agencies, Member States, etc.)
- Coordination of awareness actions, targeting entities and the general public
- Coordination of education, information and training actions for executives

5.2 NATIONAL CERT (NATIONAL INTELLIGENCE SERVICE, NIS) – NATIONAL AUTHORITY FOR MITIGATING CYBER ATTACKS

In accordance with the provisions of Presidential Decree Nr. 96/2020 (A '232) amending the provisions of Presidential Decree Nr. 1/2017 (A '2) concerning the reform of the National Intelligence Service (NIS), NIS's Cyberspace Directorate is the competent authority for:

a) Information security technical issues (INFOSEC National Authority) and particularly for the security of national communications, information technology systems, along with the evaluation and certification of classified communications and information security devices and systems

b) The evaluation and certification of cryptosystems, and the support of the Hellenic Armed Forces and public sector entities in matters of cyber security (National Authority CRYPTO)

c) The safeguarding of national electronic telecommunications equipment against infiltration, due to unwanted, electromagnetic and other transmissions (National Authority TEMPEST)

d) The mitigation of cyber-attacks against public entities participating in the national Cybersecurity network as defined by the National Cyber Security Authority, with the exception of those that fall within the competence of the Cyber Defence Directorate (CSIRT) of the National Defence General Staff.Specifically, the NIS National CERT, supports the Prime Minister's Office and the ministries, (with the exception of the Ministry of National Defense), in the prevention, early warning and response to cyber-attacks

5.3 CYBER DEFENCE DIRECTORATE (MINISTRY OF NATIONAL DEFENCE - HELLENIC NATIONAL DEFENCE GENERAL STAFF)

The Cyber Defense Directorate of the Hellenic National Defence General Staff, is the National Computer Security Incident Response Team (CSIRT), having the mission to mitigate military sector - cyber defence incidents (military CSIRT), respond to incidents against entities falling within the scope of Law 4577/2018 (OES, DSP) and the operational cooperation. The overarching mission of the Directorate is to reduce the risk emanating form national cyber security and communication challenges.

5.4 CYBERCRIME DIVISION (HELLENIC POLICE)

The Cyber Crime Division was established by Presidential Decree Nr. 178/2014 (A '281), in Athens, and maintains a Sub-Division, situated in Thessaloniki. The Division's mission includes the prevention, investigation and suppression of antisocial behaviours and crimes committed through the internet or other electronic means of communication. The Cyber Crime Division is a separate central Unit, which reports directly to the Chief of the Hellenic Police. It consists of five departments which cover all aspects of user protection and cyberspace security.

Its newly upgraded structure consists of the following Departments:

- Administrative Support and Information Management Unit
- Innovative Actions and Strategy Unit
- Electronic & Telephone Communications and Software & Copyright Protection Unit
- Minors' Online Protection and Digital Investigation Unit
- Special Cases and Online Financial Crimes Prosecution Unit

5.5 HELLENIC DATA PROTECTION AUTHORITY (HDPA)

The Hellenic Data Protection Authority (HDPA) is a constitutional independent authority, with the mission to supervise the implementation of the General Data Protection Regulation, the Law 4624/2019, the Law 3471/2006 and other legislation concerning the protection of the individual from the processing of its personal data, while exercising the rest of the responsibilities assigned to it according to its operating framework. The HDPA is responsible for monitoring the implementation of the General Data Protection Regulation (EU) 2016/679 (GDPR) provisions so as to protect the fundamental rights and freedoms of individuals against the processing of their data and to facilitate free movement of data in the Union (article 51 par. 1, recital 123 of the GDPR). It also contributes to the coherent implementation of GDPR throughout the Union by cooperating with the supervisory authorities of other Member States and the Commission (Article 51 (2), recital 123 of the GDPR).

According to the above context, the HDPA, among others:

- Monitors and enforces the implementation of the GDPR
- Promotes public awareness on personal data protection issues among the public, as well as the controllers and processors regarding their obligations according to the GDPR provisions. Special attention is paid to the activities aimed specifically at children
- Advises the Parliament, the Government, other institutions and agencies on legislative and administrative measures that are related to the protection of personal data
- Provides, upon request, information to data subjects regarding the exercise of their rights
- Handles complaints concerning the violation of GDPR provisions

- Conducts research on the implementation of the GDPR
- Compiles and maintains a catalogue in relation to the requirement for data protection Impact Assessment (Article 35 par 4 of the GDPR) and provides advice on the processing operations of article 36 par. 2 of the GDPR
- Approves codes of conduct and certification criteria, and designs accreditation criteria
- Cooperates with other supervisory authorities by exchanging information and providing assistance in order to ensure the coherent implementation of the GDPR
- Contributes to the activities of the European Data Protection Board (EDPB)
- Has audit competences, as well as corrective, advisory and authorisation powers, as specified and analysed in Article 58 of the GDPR

5.6 HELLENIC TELECOMMUNICATION & POST COMMISSION (EETT)

The National Telecommunications and Post Commission (EETT), is an Independent Administrative Authority, that monitors, regulates and supervises: (a) the electronic communications market within which fixed and mobile telephony, wireless and internet access providers operate; and (b) the postal services market, within which postal and courier services providers. Moreover, EETT is the sector specific Competition Authority being responsible for the implementation of competition legislation in these markets (L.3959 / 2011 (A '93), articles 101/102 TFEU and Council Regulation 1/2003 EC). EETT's exclusive competences regarding the implementation of competition law in the respective markets are foreseen by L.2867 / 2000, the subsequent L.3431 / 2006, and the current L.4070 / 2012 (Government Gazette 82A / 2012). EETT's position in the Ecosystem of Communications and Information Technology and its relations with the State are summarised in the following figure:

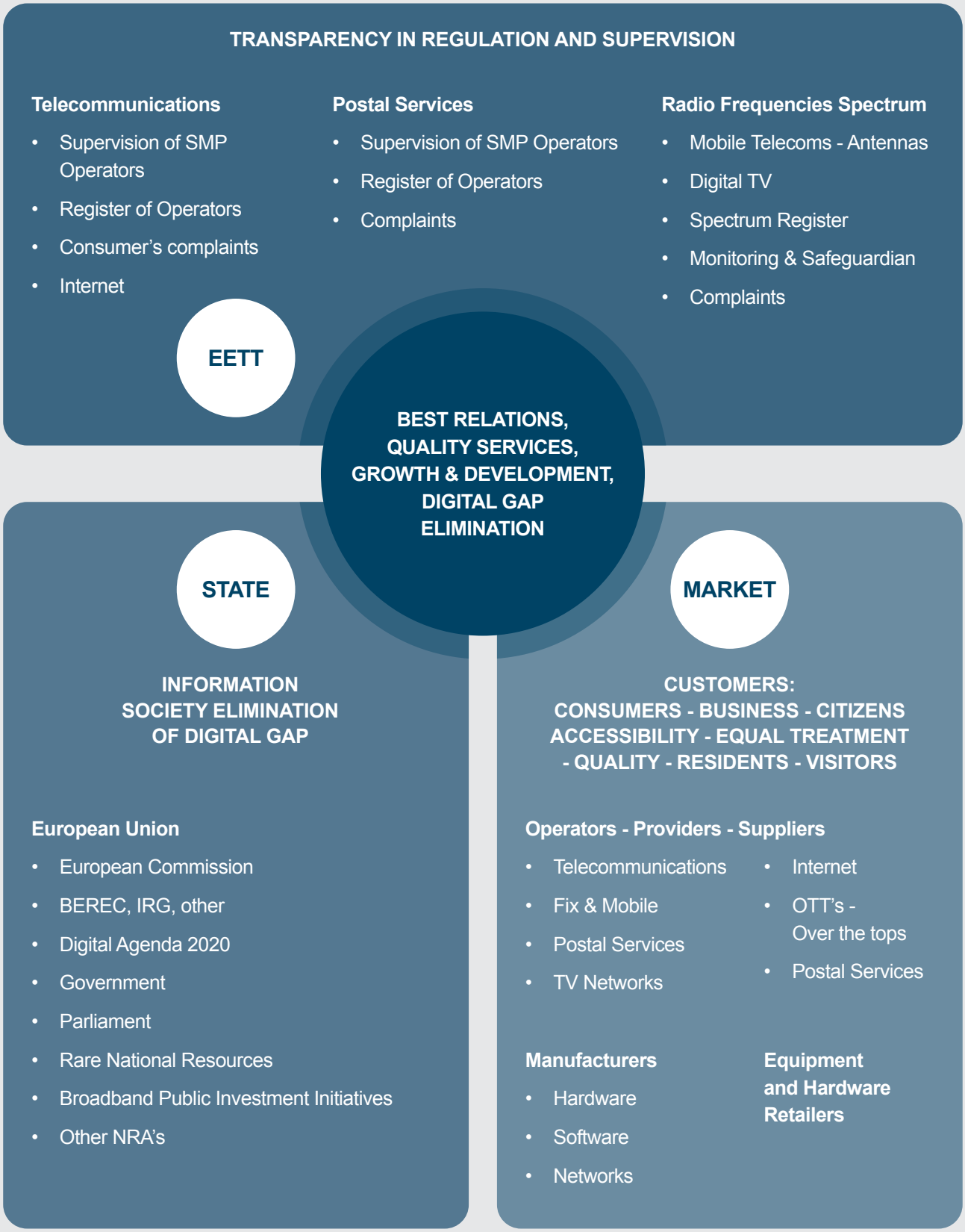

Figure 9 *EETT 's position in the Communications and Information Technology Ecosystem and its relations to the State (Source: https:/www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/)*

5.7 HELLENIC AUTHORITY FOR COMMUNICATION SECURITY AND PRIVACY (ADAE)

The Authority for Communication, Security and Privacy (ADAE) aims to protect mail confidentiality and free correspondence or communication of any other kind as well as the security of networks and information systems. ADAE is a constitutional independent authority that enjoys administrative autonomy. Its headquarters are found in Athens, but has the powers to establish and operate offices in other cities in Greece. ADAE' s decisions are communicated to the Minister of Justice, and a yearly Report of its activities is submitted to the President of the Parliament, the Minister of Justice, the leaders of the national parliamentary parties and the European Parliament.

The main responsibilities of the ADAE are the following:

- Conduct of regular and special audits in public service facilities or private companies dealing with postal, telecommunication and other services
- Legality review of the conditions and the procedures that are followed during the application of "lifting of confidentiality" provisions, in accordance with the applicable legislation
- Holding of hearings of electronic communications and postal services providers for the purpose of identifying possible violations of the applicable legislation to ensure the confidentiality of communications
- Administrative sanctions imposition in cases of confidentiality of communication violations
- Adoption of regulatory and other necessary acts regarding the applicable measures to ensure the confidentiality of communications
- Issuance of opinions, recommendations, and suggestions on issues within the Authority's competence
- Examination of complaints for violation of the confidentiality of telephone, internet and postal services communications

5.8 CENTER FOR SECURITY STUDIES (KEMEA)

The Centre for Security Studies (KEMEA) is a scientific, advisory and research organisation. Its principal purpose is the conduct of theoretical and applied research on security policy particularly at a strategic level. It also provides advisory and consulting services to an array of public and private organisations on various security issues.

It is a legal person governed by private law, under the supervision of the Minister of Citizen Protection. To fulfil its goals, KEMEA:

a. conducts research programs and studies on issues of internal security related to the Ministry of Civil Protection (formerly Public Order and Civil Protection) and the services under it, as well as other entities

b. prepares and carries out research programs as a representative of the bodies supervised by the Ministry of Civil Protection (formerly Ministry of Public Order and Citizen Protection), on behalf of or in cooperation with relevant institutions of the European Union, other states, or international organizations in accordance with the relevant rules and procedures

c. develops cooperation at national and international level with organizations and services, research and educational centres and institutions, social, scientific, and productive agencies, both public and private ones, as well as with NGOs

d. studies the criminal phenomenon and the qualitative and quantitative changes of crime in the Greek Territory and its geographical distribution, as well as the design of methods and practices in the exercise of anti-crime policy

e. proposes the harmonization of measures for the prevention and suppression of crime with constitutional principles, civil and political rights, the rule of law and respect for human dignity

f. monitors and studies the technological developments of security systems and evaluates the new achievements in this field

g. formulates proposals for the utilization of the know-how

h. supports cross-border cooperation procedures

i. organizes and conducts conferences, publishes research and general scientific findings and related projects, conducts training seminars, provides certified training in security issues and prepares certified studies in such matters

j. develops any other activity related to its goals and

k. is a certification agency for procedures, studies, security plans, bodies, organizations and companies of the Private and Public Sector

5.9 OTHER STAKEHOLDERS

Alongside the above-mentioned stakeholders, other key players include:

- The Ministries, as executive political-administrative structures forming and implementing governmental work. In addition to Ministries that have a horizontal character (e.g. Ministry of Interior, Ministry of Finance), sectoral Ministries also play an important role, since they develop particular policy areas of paramount importance to the overall functioning of socio-economic life (e.g. Ministry of Environment and Energy, Ministry of Infrastructure and Transport, Ministry of Education and Religions).

- OES / DSP Agencies, according to Law 4577/2018 and Ministerial Decision No. 1027/2019 (B ’3739) framework.

Strategic Goals	Specific Objectives	B major Stakeholders
1. A functional cybersecurity governance system	**1.A.** Optimize Organisational structures and Procedures	National Cybersecurity Authority (NCSA), central administration bodies, National CERT, CSIRT GEETHA/Cyber defence directorate
	1.B. Apply vigorous risk assessment and effective contingency planning	NCSA, central administration bodies, OES/ DSPs, CSIRT GEETHA/ Cyber defence directorate, National CERT, KEMEA
	1.C. Strengthen national, European and international collaborations	NCSA, Ministry of Foreign Affairs, National CERT
2. Shielding Critical Infrastructures and securing new technologies	**2.A.** Comprehend technological developments and their effects on digital governance	NCSA, Research and scientific organizations, ADAE., EETT., General Secretariat for Research and Technology, Ministry of Foreign Affairs, National CERT
	2.B. Upgrade critical infrastructures’ protection	NCSA, OES/DSPs, CSIRT, GEETHA/ Cyber defence directorate, National CERT
	2.C. Consolidate systems and applications by implementing enhanced security requirements	NCSA, central administration bodies, OES/DSPs, CSIRT, GEETHA/ Cyber defence directorate, National CERT, KEMEA
3. Incident management optimisation, fight against cybercrime and privacy protection	**3.A.** Optimise methods, techniques and tools utilised in incident analysis, response and reporting	NCSA, Cyber defence directorate, National CERT,. Hellenic Police – Cybercrime division
	3.B. Strengthen deterrence mechanisms and enhance operational cooperation	NCSA, GEETHA/ Cyber defence directorate, National CERT, Hellenic Police – Cybercrime division
	3.C. Cybersecurity for the protection of privacy	NCSA, Hellenic Data Protection Authority(HDPA), ADAE
4. A modern environment for cybersecurity investments with emphasis on the promotion of Research and Development	**4.A.** Encourage R&D initiatives	NCSA, General Secretariat for Research and Technology, Ministry of Development and Investments, Ministry of Finance, Center for Research and Technology/NIS
	4.B. Provide investment incentives	NCSA, Ministry of Development and Investments, Ministry of Finance
	4.C. Utilise PPPs	NCSA, Ministry of Development and Investments, Ministry of Finance
5. Capacity building, promoting information and awareness raising	**5.A.** Building capacity by organising cybersecurity excersising activities	NCSA, GEETHA/ Cyber defence directorate, Hellenic Police – Cybercrime division, National CERT
	5.B. Apply state - of - the - art educational and training methods and tools	NCSA, Ministry of Education and Religious Affairs, Research and scientific organizations
	5.C. Promote open - ended cybersecurity information and awareness raising for Entities and citizens	All relevant stakeholders, citizens, companies

Figure 10 *Key stakeholders by Strategy and Specific Objective of the National Cyber Security Strategy 2020 - 2025*

6 CRITICAL SUCCESS FACTORS

6.1 S.W.O.T. ANALYSIS

The implementation of the National Cybersecurity Strategy is on the one hand inextricably linked with the operation of the General Directorate of Cyber Security, on the other hand with its implementation by the stakeholders. In order to adequately analyse the internal and external factors that will contribute to the successful implementation of the Strategy and ensure the provision of secured services to citizens, the Strengths, Weaknesses, Opportunities and Threats, are summarised by performing a SWOT analysis as exhibited in the following table:

Strengths	Opportunities
• Commitment of the Ministry of Digital Governance, as well as of the Greek Government, concerning the development and implementation of the National Cyber Security Strategy • Expertise of the NCSA executives and flexible procedures • Specialisation of entities (both public, such as GEETHA / Cyber Defence Directorate, NIS agency, and private) in cyber security	• Implementation of a national digital governance strategy, which introduces the concept of cyber security by design and by default • Public and Private Partnerships (e.g. through PPPs) which can assist the NCSA in its work

Weaknesses	Threats
• Incentives to attract and retain staff with appropriate - high technical qualifications • Financial constraints and complex procurement and service procedures • Fragmentation and complexity of structures and procedures - coordination challenges	• Operation methods (modus operandi) of attackers and threatening factors, which are incompatible with any administrative or operational practice (e.g. schedule, number of executives, salary incentives, etc.) • Rapid pace of technological developments - inherent difficulties in monitoring and comprehending

Hence, the Strategy's successful implementation depends on specific critical success factors, which must be accommodated by all stakeholders, including all competent authorities.

6.2 CONDITIONS CONCERNING THE NCSA

- Adequacy of resources – staffing

  Adequate staffing of the Authority, in accordance with the applicable organisational or institutional provisions are necessary for the equivalent assumption of competences and the achievement of the Strategy's objectives. Due to the nature of the work the Authority is called upon to perform, its executive staff are required to provide specialized services, while at the same time they should be in readiness to provide work beyond the usual working hours that apply to public employees.

- Further strengthening of the regulatory framework

  In the context of the effective implementation of the NCSA's responsibilities, the importance of further strengthening the regulatory framework is crucial, through the adoption of clear and coherent legislation, taking into account Better Regulation rules and principles.

- Flexibility of partnerships through PPPs

  In cases where the Authority assesses that working into partnership with the private sector (via PPPs) will bring significant benefits to its work, the Authority should be able to partner with private entities on respective flexible terms.

- Sufficient funding for the planning, development, and implementation of actions

  Sufficient funding and allocation of resources to the Authority is necessary to support comprehensive planning, development, implementation and monitoring of the Strategic plan's actions.

- Proper equipment

  For the fulfilment of the Authority's mission and responsibilities, it is also considered necessary to strengthen it with modern equipment, logistical infrastructure and facilities.

6.3 CONDITIONS CONCERNING THE ENTITIES

- Investment incentives. One of the Strategy's main objectives, is to strengthen investment programs in cybersecurity by the private sector and other interested entities. Appropriate incentives (e.g. financial - tax relief) should be provided to promote public and private sector investment in cybersecurity.

- Incentives for cooperation. At the same time, appropriate incentives should be provided to facilitate cooperation between public / private sector and educational institutions, to promote the objectives of working

with private actors who can provide critical information and services to the Authority, to support research and development in the field of cyber security, as well as to strengthen the implementation of training programs.

7
STRATEGIC GOAL 1: A FUNCTIONAL CYBERSECURITY GOVERNANCE SYSTEM

7. 1 SPECIFIC OBJECTIVE 1.A.: OPTIMIZE ORGANISATIONAL STRUCTURES AND PROCEDURES

A fundamental priority for the implementation of the National Cyber Security Strategy, consists the development of an integrated "Greek cyberspace" system of governance, under the coordinating role of the Authority, in which:

All areas of cyber security intervention are addressed holistically[6]

Clear roles and responsibilities are defined for all stakeholders

Clear, pre-defined procedures are foreseen, based on which the governance system is organized, and on which it operates and evolves.

In the light of the above principles, a system having the National Cyber Security Authority as a lead agency is formed, involving a network of agencies and security officials at the level of: a. preventive actions and b. response and operational continuity:

KEY SECTORS IN LAW 4577/2018 (OES-DSP)

Energy (Ministry of Environment and Energy, OES - DSP)
Transport (Ministry of Infrastructure and Transport, OES - DSP)
Banks (Ministry of Development and Investment – Bank of Greece, OES - DSP)
Stock market infrastructures (Ministry of Development and Investment, OES - DSP)
Health sector (Ministry of Health, OES - DSP)
Drinking water supply and distribution (Ministry of Infrastructure and Transport, OES - DSP)
Digital infrastructure (IXP, DNS, TLD) (Ministry of Digital Governance - EETT - OES - DSP)

KEY SECTORS (EXCEPT LAW 4577/2018)

Telecommunications (Ministry of Digital Governance, EETT, ADAE)
Justice (Ministry of Justice, Judiciary)
Education (Ministry of Education and Religious Affairs)

[6] It is noted that from the above framework classified Communication and Informatics Systems (ITS)are excluded, in accordance with the National Security Regulation

PUBLIC SECTOR – PUBLIC ADMINISTRATION

Central Public Administration (Law 4622/2019, A' 133):

a. The Presidency of the Hellenic Republic

b. The Presidency of the Government

c. Ministries and their decentralised or regional services

d. Decentralised Administrations, and

e. Independent Authorities

First and second level Local Government Authorities

Other entities of General Government (Legal persons governed by public law, Legal persons governed by private law, public companies, public enterprises, etc.)

PRIVATE SECTOR

Citizens' services

Businesses

Civil society

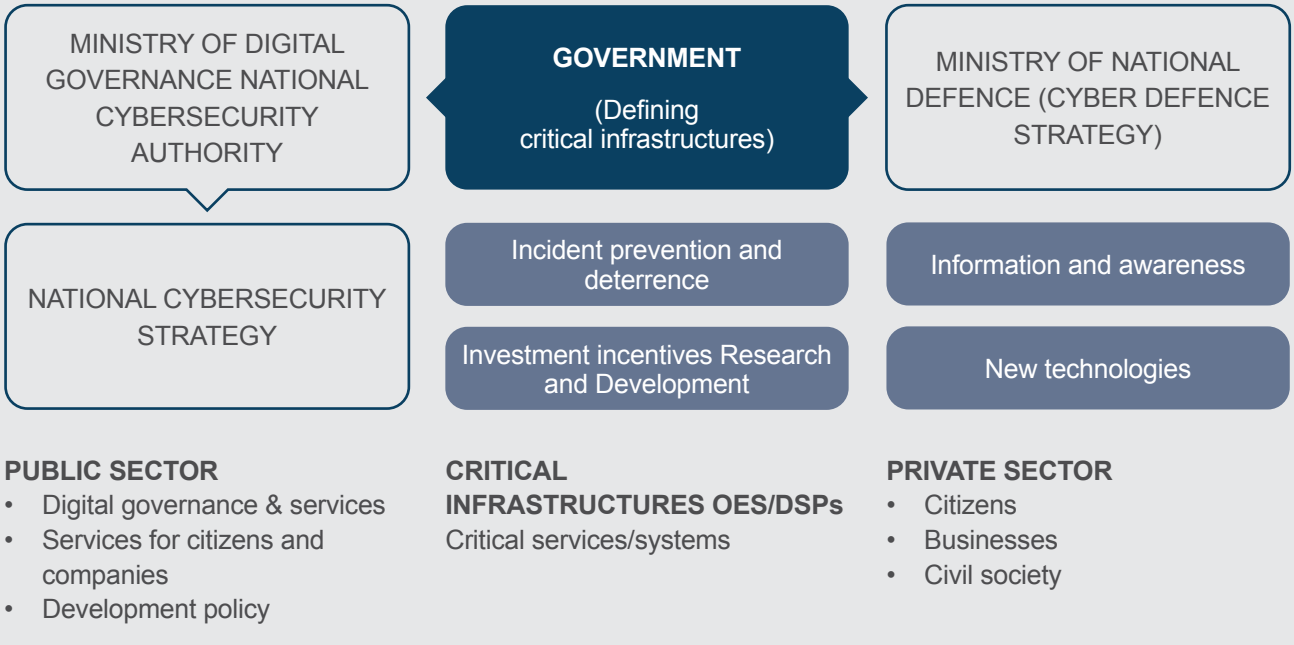

Figure 11 *Governance framework of the National Cybersecurity Strategy 2020 - 2025*

In particular, the flagship initiatives of this specific objective include, inter alia:

7.1.1 Development of an integrated cybersecurity management system for public entities

In order to optimize the governance and increase the cybersecurity of public systems and networks, a critical action is the development of a comprehensive cybersecurity management framework for public entities so that:

- Incidents are prevented and responded
- The most modern technology in public infrastructure and services is utilised in a secure manner
- Knowledge of ways to shield network and information systems is disseminated promptly and in a timely manner

In this light, the following are considered as key priorities:

- Functional reorganization - strengthening of IT and e-government services
- Appointment of Information Systems and Networks Security Officers
- Centralised issuance of instructions, directions, alerts, and security requirements by the National Cyber Security Authority
- Upgrading the security design of information systems and networks of public entities on the basis of risk analysis methodology
- Upgrading CERT to optimise response and incident management

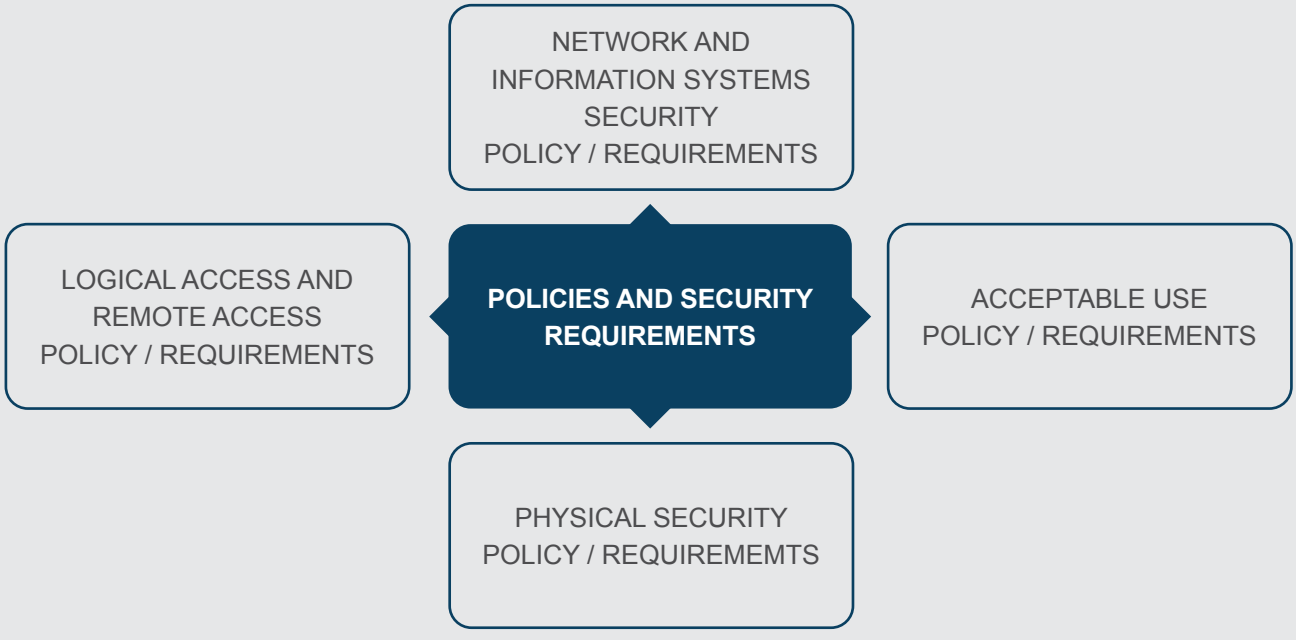

Figure 12 *Policies and security requirements for public entities*

7.1.2 Cybersecurity excellence management framework

An additional flagship initiative is the formulation and implementation of an integrated framework for the promotion of excellence in the field of cyber security. In particular, under this framework, international and European good practices will be collected in a Cybersecurity Handbook containing recommendations and instructions, so that organisations can easily and quickly take immediate measures to strengthen their level of cybersecurity. This handbook will be accompanied by a self-assessment tool, as well as by a system of identification and incentivisation, through which the highest performing agencies will be foregrounded.

7.2 SPECIFIC OBJECTIVE 1B: APPLY VIGOROUS RISK ASSESSMENT AND EFFECTIVE CONTIGENCY PLANNING

Effective protection against threats that may affect the provision of services to citizens presupposes the identification and registration of these threats. The identification of cyber security threats is based on a methodology developed for this purpose, which promotes cooperation with agencies such as the National Intelligence Service, the Hellenic National Defence General Staff (GEETHA), and the European Information and Network Security Agency (ENISA). Fundamental interventions in the context of this objective are the development of a data analysis and threat logging methodology, the formulation of a national risk assessment plan and the national emergency plan.

In particular, the flagship initiatives of this specific objective include, inter alia:

7.2.1 Risk assessment and development of a National Risk Assessment Plan

Cyber security risk assessment and effective risk management constitute one of the main pillars of cyber security and digital governance. For the purpose of risk assessment/risk management, key priorities constitute the following:

- Defining a specific framework under which Agencies will identify critical operational activities and the information resources that support them
- Defining a specific framework under which Agencies will identify external and internal factors that may affect the security of information resources
- Profiling of threats and assessing the vulnerabilities these threats may exploit
- Establishing a cybersecurity risk management plan

Key action also constitutes the preparation of a national risk assessment study, by following a scientific process that is concisely based on the identification, analysis and assessment of risk impacts and will eventually lead to the definition of a critical infrastructure protection plan by sector and / or entity. The study, which will be reviewed at least every three years, will take into account all possible threats, especially those related to malicious

actions (e.g. cybercrime, cyberattacks), but will also include the risks associated with natural phenomena, technical failures, malfunctions and human mistakes. Furthermore, threats arising from the interdependence between communication and information systems of the actors involved in the National Strategy will be taken into account, especially those regarding critical infrastructures, while the extent and the criticality of the effects at national level will be further evaluated.

7.2.2 Development of a National Contingency Plan

The aforementioned actions will also contribute to the development of a National Contingency Plan, while they will facilitate the classification of the Entities according to their offered services and their compliance with current legislation and regulations (such as NIS Directive and Law 4577/2018).

The National Contingency Plan is the guide for dealing with incidents that are deemed to be serious disruptions to the services provided by the Entities and falls into the realm of crisis management. Therefore, the Plan includes the criteria according to which an event is categorised as a crisis, the roles related to crisis management and their respective responsibilities, as well as the actions that should take place to successfully deal with the event, while activating all appropriate safeguards that will mitigate the effects and prevent service interruptions. The National Contingency Plan is activated to respond to events that cause serious disruption to the provision of services by theentities, or endanger the general provision of services to citizens. Such incidents are referred to as crises, with the Plan being the crisis management manual.

The National Contingency Plan includes the following:

- **Definitions (crisis management, operational continuity)**

  All crisis management definitions are included, so that stakeholders can align with the used terminology and develop a common working language.

- **Criteria**

  Criteria that define when an event is considered a crisis and / or requires the activation of the National Contingency Plan.

- **Scenarios, roles, and responsibilities**

  Description of scenarios that fall under the definition of crisis, based on the aforementioned criteria.

  Listing of roles and key stakeholders, as well as their responsibilities in a state of readiness, activation of the Plan and recovery.

  Description of actions during a crisis.

- **Linking with operational continuity and disaster recovery plans**

  Listing of correlations with operational continuity and disaster recovery plans to facilitate the resolution of a crisis and to carry out the necessary actions for recovery and return to normalcy.

  Technologies and resources for recognition, response and recovery.

- **Assessment, analysis and identification of vulnerabilities / risks**

  Listing the results of a cyber security risk assessment that may lead to a crisis.

- **Identify Crisis signals**

  Methodology for early recognition of an impending crisis, aiming at the immediate activation of the Plan.

- **Communication for crisis management (communication between Entities, relationship management, communication with the media, communication with competent Ministries, etc.)**

  Contact details, prepared messages, distribution of roles.

- **Exercise options**

  Exercise analysis

  Indicative scenarios

  Exercise plan

7.2.3 Utilization of modern information exchange mechanisms

The exchange of information between the private entities participating in the National Cybersecurity Strategy and their public oversight entities including the National Cybersecurity Authority, is of particular importance for the implementation of the National Strategy. Private entities are invited to exchange information on the communication and information systems they operate, the security policies they have implemented, the vulnerabilities, threats and security incidents they face. Accordingly, public agencies are required to exchange information gathered by the relevant entities, which may jeopardize the desired level of cybersecurity. By correlating this information, it is possible to analyse the evolution of the threats related to cybersecurity at national level. It is necessary to develop those mechanisms for the reliable exchange of information within a framework of mutual trust and respect for the role and responsibilities of all stakeholders involved in the National Cybersecurity Strategy.

7.3 SPECIFIC OBJECTIVE 1.C.: STRENGTHEN NATIONAL, EUROPEAN AND INTERNATIONAL COLLABORATIONS

Modern technologies have contributed to the development of a strongly interconnected environment without borders. In order to safeguard common interests, cyber-diplomacy is used to promote responsible cyber-behaviour at the state level. In parallel, cross-border dependencies require international cooperation, with the aim of achieving a common high level of security. In this context, our country must maintain and strengthen its participation in in the international cooperation spectrum, aiming at:

- Ensuring cooperation for the joint development of means as to mitigate threats and incidents
- Building and strengthening alliances to jointly counter cyber-attacks
- Ensuring access to information and know-how
- Jointly formulating legislative proposals at European level
- Jointly implement decisions adopted within the framework of international organisations, in which Greece participates

In particular, the activities of this specific objective include:

- Reinforce the Greek presence and participation in international alliances on cybersecurity issues.
- Support cooperation with third countries in the bilateral transfer of know-how, with the aim of achieving a common high level of security and dealing more efficiently with cross-border threats.
- Establish a method for determining anticipated cooperation on cybersecurity issues and conclude cooperation agreements with third countries. Create a management model to facilitate progress in cooperation initiatives in order to enhance the national level of security, develop skills and build awareness through cooperation.

7.4 FLAGSHIP ACTIVITIES

Objectives	Activities	Milestones
1.A. Optimize Organisational structures and Procedures	**1.A.1.** Development of an integrated cybersecurity management system for public sector entities	Q2 2021
	1.A.2. Development of a framework for the promotion of cybersecurity excellence management	Q3 2022 - Continuous activity
	1.A.3. Drafting of sectoral action plans (e.g. Energy, Healthcare, Transport, Finance, Telco, Maritime, etc.)	Q4 2024
	1.A.4. Reinforcement of information sharing mechanisms	Q2 2022
1.B. Apply vigorous risk assessment and effective contigency planning	**1.B.1.** Development of a data analysis methodology and a threat Registry	Q4 2021
	1.B.2. National risk assessment planning	Q4 2021 - Continuous evaluation and update
	1.B.3. National contingency planning	Q4 2021 - Continuous evaluation and update
1.C. Strengthen national, European and international collaborations	**1.C.1.** Strengthening the Greek presence and participation in international alliances on cybersecurity issues	Continuous activity
	1.C.2. Support for cooperation with third countries in the bilateral transfer of know-how with the aim of strengthening the common high level of security and efficiently responding to cross-border threats	Continuous activity
	1.C.3. Establishing a methodology for international collaborations on cybersecurity issues and conclude cooperation agreements with third countries	Q4 2021 - Continuous activity
	1.C.4. Creation of a management model to facilitate progress in cooperation initiatives in order to enhance the national level of security, develop skills and build awareness through cooperation	Q4 2021 - Continuous activity

8
STRATEGIC GOAL 2: SHIELDING CRITICAL INFRASTRUCTURES AND SECURING NEW TECHNOLOGIES

8.1 SPECIFIC OBJECTIVE 2.A.: COMPREHEND TECHNOLOGICAL DEVELOPMENTS AND THEIR EFFECTS ON DIGITAL GOVERNANCE

The digital transformation of Public Administration and the provision of electronic services to the citizens are inextricably linked to technology, as well as to the developments in the field of ICT (such as 5G, IoT, Artificial Intelligence, etc.). These technologies, on the one hand, influence the structure of digital governance by providing appropriate tools to serve citizen's demands promptly and reduce bureaucracy, and, on the other hand, require the adoption of cybersecurity principles by design and by default to ensure the protection of infrastructure and data and compliance with existing laws and regulations (for instance EU GDPR7 και 4624/20198, NIS Directive9 και 4577/201810, ePrivacy11, etc.)[7, 8, 9, 10, 11].

More specifically, the flagship activities of this specific objective include, inter alia:

8.1.1 Cyber security of 5th generation (5G) networks

Within the framework of European coordination and cooperation concerning the protection of the cybersecurity of 5G networks, the European Commission issued Recommendation No. 2019/534 to the Member States, the relevant institutions - bodies and other EU bodies, as well as the cooperation group set up under Directive (EU) 2016/1148 (NIS Cooperation Group). In accordance with this Recommendation, the necessary steps for a unified approach to address cyber security risks of 5G networks were identified: a. conducting national risk assessments, b. developing a European risk assessment, c. developing a European toolbox with risk mitigating measures (5G Cybersecurity Toolbox), and d. implementing measures of the toolbox.

[7] *bit.ly/3ks3SIR*

[8] *bit.ly/37S9U0l*

[9] *bit.ly/2Mu13ut*

[10] *bit.ly/30559w0*

[11] *bit.ly/3qYqbsn*

The main content of the measures is related to the implementation of strategic and technical measures. Key issues concern security procedures of the 5th generation (5G) networks and equipment, as well as the diversification of 5G equipment suppliers. The proposed measures are summarized below:

Strategic measures:	
Control measures – restrictions and prohibitions	**a.** Strengthening national regulatory authorities to enforce - monitor further security measures **b.** Increasing their control role **c.** Carrying out risk analyses by providers, Member States and / or the EU itself to verify the profile of suppliers **d.** Powers to impose restrictions and / or prohibitions on the safeguarding of critical or sensitive goods (e.g. core network, network management, access control) to high-risk suppliers **e.** Powers to impose restrictions on outsourcing of operations to MSPs, including physical and virtual infrastructure **f.** Foreign Direct Investment Control (FDI) control measures
Market operation measures	**a.** Ensuring that each MNO has an appropriate strategy to avoid dependencies on a single supplier **b.** Providing diversification of suppliers within the market **c.** Utilizing EU (and national) mechanisms for policy and strategic investment in innovation, research and new technologies with the specific aim of promoting sustainable operation throughout the 5G value chain
Technical measures:	
Security policies for MNOs	**a.** Ensure the implementation of the basic security requirements **b.** Ensure that providers and their suppliers implement the security measures provided in the 5G standards **c.** Ensure strict access controls **d.** Enhance the security of virtual network operations **e.** NOC - SOC security, monitoring and operation of the network **f.** Strengthen physical security **g.** Enhance software security **h.** Ensure resilience and continuity **i.** Control of security standards of suppliers at the stage of supply by providers
Promoting a certification system at EU level	**a.** In the first stage for network systems / customer equipment related to 5G **b.** Next step, possibly for 5G-related equipment suppliers **c.** Use EU certification for other 5G-related ICT products and services (connected devices, cloud services)

8.1.2 Industrial Internet of Things

As part of this activity, the National Cybersecurity Authority will collect data that reflect the degree of integration of Industrial Internet of Things technologies on existing SCADA systems. SCADA systems are industrial control systems and compose the core of the implementation of basic services (eg distribution, transportation, refining, etc.) by OES that perform industrial processes. These are legacy systems that have been around for decades.

Industrial Internet of Things refers to technologies such as connected sensors and other devices, which network with existing industrial systems and introduce new channels for the exchange of information between interconnected stations and the Cloud, thereby increasing the attack surface and the consequent need to implement specialized security measures.

8.1.3 Artificial Intelligence

Artificial intelligence enables machines to “understand” their environment, solve problems, and act toward a specific goal. The computer receives data (already prepared or collected through sensors), processes it and responds based on it. This new environment introduces new threats and innovative ways of attacking these systems, such as the introduction of corrupted data into corporate machine learning algorithms in order to make the wrong decisions, with dangerous consequences. Also, machine learning algorithms can be used by the attackers themselves in order to produce more advanced malware that can bypass network intrusion detection systems. As part of this activity, the National Cyber Security Authority will develop specialized security measures to protect artificial intelligence systems from attacks.

8.2. SPECIFIC OBJECTIVE 2.B: UPGRADE CRITICAL INFRASTRUCTURE PROTECTION

The Authority will provide support to public administration bodies and other stakeholders for the effective protection of critical infrastructure, in areas such as the implementation of basic principles and requirements of cybersecurity, the control and evaluation of Entities, the conduct of technical security checks, and the regular evaluation of the Entities through the appropriate audits. Fundamental interventions under this objective concern the development and implementation of an integrated coordination framework for CISOs, the development of specific practices for the detection, quantification, prioritization, early warning and risk management of critical infrastructure, and the development of threat landscape reports. Furthermore, in the context of optimizing the evaluation and feedback of security planning for critical infrastructure, a key action is the creation of standard questionnaires so that Entities are able to capture their current level of maturity and readiness to respond to security events and comply. with the provisions of the current legislation.

Figure 13 *Maturity model for the evaluation of actors based on the level of cyber security*

- The questionnaire contains the minimum required measures that a body must take
- The performance of the maturity levels aims to record the current situation, so that the Entity can take appropriate measures to improve the existing cybersecurity framework
- The lower the level of maturity, the greater the risk of exploiting weaknesses by threatening factors

8.3 SPECIFIC OBJECTIVE 2.C.: CONSOLIDATE SYSTEMS AND APPLICATIONS BY IMPLEMENTING ENHANCED SECURITY REQUIREMENTS

The effective systems and applications shielding, in the context of a comprehensive assessment of the threat and risk factors, presupposes the formation of a coherent and applicable framework of appropriate security requirements. Key parameters in this design are the development and management of a hardware / infrastructure, software as well as intangible information assets registry in critical sectors (public, critical infrastructure), the entities categorization to determine enhanced security requirements, the need of issuing enhanced security requirements (horizontal and sectoral) taking into account international and European certification standards and frameworks.

At the same time, in order to effectively comply with the security requirements, it is necessary to develop an audit system (for the implementation of security requirements),as part of which reports with findings and recommendations will be prepared. In particular, the flagship activities of this specific objective include, inter alia:

8.3.1 Development and management of a hardware, software and intangible information assets registry

As part of this action, National Cybersecurity Authority will take action in:

- Recording in an appropriate and up-to-date list (registry) of all the resources required for the provision or support to the basic services of OES and DSPs
- Ensuring the resilience of the systems that support basic services against threats, by implementing the appropriate test procedures and technical audits of OES and DSPs, in cooperation with the relevant competent entities
- Carrying out the necessary audits to ensure software and applications protection of OES and DSPs din the areas of responsibility of the Cyber Security, in accordance with security requirements (especially operating systems, applications, database management systems, PCI applications, COTS), and in cooperation with the competent entities on a case-by-case basis
- Carrying out audits to ensure networks, hardware and systems protection of OES and DSPs in accordance with security requirements (intrusion prevention / detection) in cooperation with the competent entities, as the case may be
- The definition and categorization of information assets and the maintenance of a relevant repository registry in cooperation with the relevant entities, as appropriate
- The issuance of guidelines and instructions regarding Cybersecurity for the protection of information assets, in accordance with security

requirements (including privacy and data protection requirements, encryption, PKI, backup, DLP, data retention / destruction)

- Providing support for the protection of the network perimeter, in accordance with the security requirements (firewalls, DMZ, network connections, third party connection, remote access, VPN, etc.) in cooperation with the relevant competent entities

8.3.2 Issuance of security requirements

The National Cybersecurity Authority will set the minimum security requirements and the corresponding technical and organizational measures, based on the risk assessment at national level, that the entities must implement in order to achieve a fundamental and common level of security. In this light, it is considered necessary to establish a minimum, common and harmonized level of requirements and measures between the entities, which will be applied during the implementation, evaluation and audit of proper implementation. Furthermore, the possibility of exchanging information between entities is strengthened, as there is a “common language”, while also facilitating the reporting of security incidents and the implementation of common security practices.

Consequently, stakeholders are required to implement specific cybersecurity measures to ensure the protection of their information resources. Due to the nature of each Agency and the regulatory requirements that may govern its operation, the Authority will define the basic principles and requirements to be met (cyber security baselines) depending on their categorization. These measures include measures to prevent and deal with security incidents. Cyber security requirements will facilitate the definition of a single framework for the protection of Entities, as well as the effective control of their implementation. At the same time, they will constitute the basis for the issuance of standards and circulars by the Authority, the establishment and monitoring of indicators (KPIs, KRIs), the revision based on developments in ICT and directives by national and European bodies, as well as the coordination of Entities in responding to cybersecurity incidents.

8.3.3 Development of a cyber security audit system

In order to increase the protection of the relevant entities, the National Cyber Security Authority will undertake:

- The formulation and elaboration of an audit program regarding the implementation of the National Strategic Cyber Security Plan

- Carrying out regular and ad hoc audits of the facilities, equipment and technological infrastructure by Audit Teams set up by the National Cybersecurity Authority by drawing up relevant reports indicating the necessary corrective interventions and monitoring their implementation, in cooperation with the competent entities, where appropriate

- The preparation of reports on information and network security audits
- Ensuring the adequacy of controls to meet security policies, standards and requirements
- Ensuring the adequacy of controls over compliance with the requirements of confidentiality, privacy and protection of personal data
- Making recommendations and suggesting measures and actions to improve the implementation of the strategic planning for Cybersecurity

8.4 FLAGSHIP ACTIVITIES

Objectives	Activities	Milestones
2.A. Comprehend technological developments and their effects on digital governance	**2.A.1.** Implementation of an integrated cybersecurity framework for 5G networks	Q4 2021 - Continuous activity
	2.A.2. Implementation of a framework of security measures and actions for Artificial Intelligence	Q4 2021 - Continuous activity
	2.A.3. Implementation of a framework of security measures and actions for the Internet of Things (IoT)	Q4 2021 - Continuous activity
	2.A.4. Development of enhanced collaboration with academic and research institutions on new technologies	Q4 2021 - Continuous activity
2.B. Upgrade critical infrastructure protection	**2.B.1.** Defining and updating a list of critical infrastructures	Q4 2022
	2.B.2. Development and implementation of a coordination framework for CISOs	Q1 2022
	2.B.3. Development of practices for detection, quantification, prioritization, early warning and risk management for critical infrastructure	Q4 2022
	2.B.4. Preparation of threat landscape reports	Q4 2025

Objectives	Activities	Milestones
2.C. Consolidate systems and applications by implementing enhanced security requirements	**2.C.1.** Development and management of a hardware, software and intangible information assets registry in critical sectors (public, critical infrastructure)	Q4 2021 - Continuous activity
	2.C.2. Categorization of entities for the determination of enhanced security requirements	Q2 2023
	2.C.3. Issuance of enhanced security requirements (horizontal and sectoral) taking into account international and European standards and certification frameworks	Continuous activity
	2.C.4. Issuance of special security requirements for public ICT projects	Q4 2022 - Continuous activity
	2.C.5. Development of an audit system for the implementation of security requirements	Q4 2021 - Continuous activity
	2.C.6. Development of an integrated system for assessing the maturity level of entities	Q4 2021 - Continuous activity

9 STRATEGIC GOAL 3: INCIDENT MANAGEMENT OPTIMISATION, FIGHT AGAINST CYBERCRIME AND PRIVACY PROTECTION

9.1 SPECIFIC OBJECTIVE 3.A.: OPTIMISE METHODS, TECHNIQUES AND TOOLS UTILISED IN INCIDENT ANALYSIS, RESPONSE AND REPORTING

The knowledge of the technical details of the incidents that the entities are called to deal with, their analysis and the dissemination of knowledge is required, in order for all participants to prepare more effectively in responding to incidents but also to take the necessary corrective actions in relation to the security measures they have taken (in place so that the risk of recurrence is minimized). In this way, the preparedness and capacity to deal with security incidents and recovery after them is strengthened at national level. Critical events are managed in accordance with the National Cyber Contigency Plan. A special role in dealing with security incidents is played by Computer Security Incident Response Teams (CSIRT), whose main role is to coordinate incident handling by the stakeholders, based on defined roles, responsibilities and procedures as well as operational and communication capabilities. At national level, other computer security incident response teams relative to computer security by sector are already in operation or can be set up.

In addition, the National CERT aims to optimize the level of prevention, assessment and analysis of threats among the entities involved in the National Strategy. The National CERT, in cooperation with the other CSIRT / CERTs operating within the country but also with other national CSIRT / CERTs with which it has established a cooperation network, constantly monitors at national and international level the threats and vulnerabilities of information and communication systems, analyses and evaluates them, based on the specifics of the country, and informs the entities in order to strengthen their readiness in dealing with security incidents. In particular, the cyber security incident management framework includes definition of appropriate infrastructure, assignment of roles and responsibilities,

cyber hotline operation so that the Entities (OES and DSPs) are able to report security incidents, cooperation with bodies such as the National Intelligence Service and the Cyber Defence Directorate, use of security operations centre (SOC), elaboration of cyber security incidents instructions (operations handbook), as well as a list of other contracting third parties. In the event of a cybersecurity incident, the entities involved in the National Strategy must be prepared to respond effectively. In the light of the above, care should be taken to detect, prioritize, analyse, respond to and recover from suspicious security incidents, as well as to cooperate with the Cyber Defence Directorate, the National CERT and the N.I.S. INFOSEC as well as with other CERTs operating in Greece. In particular, the flagship activities of this specific objective include, inter alia:

9.1.1 Establishment of a Critical Infrastructure Monitoring Centre (Security Operations Centre - SOC)

It is considered necessary to develop the ability to monitor and respond to security incidents and to exchange information with the competent Entities. This capability is provided through the establishment of a Critical Infrastructure Monitoring Centre (SOC) and the establishment of a Cyber Incident Response Team (CSIRT). The operation of a Critical Infrastructure Monitoring Centre (SOC) requires the following, as a minimum:

Figure 14 *Operation SOC*

The purpose of the Centre is the continuous monitoring of the critical infrastructure of the Entities and the timely identification and handling of security incidents.

Responsibilities:

- Implementation and management of appropriate tools

  The execution of the Centre's work is based, in addition to its executives, on tools. These tools aim to collect data from log files and correlate them with a view to effective threat identification. At the same time, they allow the establishment of the Agency's network traffic profile, the definition of appropriate indicators and alerts, as well as the intervention in the network to avoid the spread of an attack or infection with malware.

- Investigation of suspicious actions in order to identify threats

  Investigation of suspicious actions is necessary to mitigate false positives, i.e. situations where legal network traffic is categorized as illegal, but also false negatives, i.e. situations where illegal network traffic goes unnoticed, categorized as legal.

At the same time, with the use of appropriate tools and procedures, the staff of the Centre can carry out the initial response actions - triage, during which it is decided whether an action needs further investigation, considered as an event or not.

Investigating suspicious activity is a critical process, especially if personal data is involved and an incident must also be treated as a breach of personal data.

- Ensuring business continuity of entities

  Through the timely recognition and prevention (or mitigation) of events, the business continuity of the Entities is ensured. At the same time, through the network traffic monitoring, the Centre will provide data to the Directorate of Prevention and Protection for the preparation of appropriate instructions to the Entities.

- Support for actions of the NCSA Directorates

  The actions of the Centre are complementary to the Directorates of the Authority, providing data for the Entities, either individually or collectively, so that there is, at all times, a picture of the situation of the Entities regarding the applied cybersecurity framework.

9.1.2 Creation of a Cyber hotline

In order to promptly and effectively deal with security incidents, it is proposed to establish appropriate communication interfaces with OES and DSPs.

More specifically, it will be created:

- Contact phone
- email address

This address / mailbox will send the message to the Centre (SOC) for further investigation. The above data fill in the incident report form already posted, in the above link.

9.1.3 SOC Infrastructure and Case Management

The Centre's (SOC) operation is also based on the use of specialized tools aimed at (a) monitoring network traffic and event recognition, but also (b) managing cases within the Centre (case management).

Core tools of a Centre (SOC) are summarized as follows:

- Security Information and Event Management System (SIEM)

One of the main tools of a centre (SOC), which aims to:

a. The collection of data from monitored devices (logs), their safe storage and analysis by Analysts as needed

b. The correlation of data (log correlation) in order to identify threats that could affect the business continuity and operation of an Entity

c. Security Orchestration, Automation and Response System (SOAR)

SIEM Systems, while a key tool for analysts to diagnose events in a timely manner, do not include, as a functionality, event response, i.e. the application or change of specific rules in the monitored systems. For these purposes, SOAR tools are used in parallel, so that response actions are automated, based on rules and direct cooperation with the SIEM system.

Due to the escalation of cyber-attacks, SOAR systems have now become necessary for a Centre (SOC). Also taking into account the lack of cyber security executives worldwide, these tools are used to fill this gap, by protecting Entities and allowing existing executives to focus on other items.

Case Management System

These systems come to cover the administrative part of the Centre 's operation. Each case that is subject to investigation is also a case which is managed by different executives, even between shifts.

This case management system aims at:

a. The effective management of each case, including a variety of data such as date and time, involved Analysts, case description, actions that have taken place and / or planned, communication results with the Entities, instructions from Engineers - SMEs, etc.

b. Monitoring the progress of a case by the Supervisors, recording the time taken to resolve the case, recording management metrics (e.g. response times, number of contacts with the Agency, etc.) and production of corresponding applications

In a modern Centre (SOC), the use of a case management system becomes imperative, with priority (several times) over a central SIEM tool.

9.1.4 Incident log development, threat intelligence tools and website protection

Furthermore, the following actions are planned in the context of optimizing methods, techniques and tools for incident analysis, response and reporting:

- Establishment and management of an incident log (formal and / or anonymous), including all information related to the event, actions taken, results, lessons learned

- Operation of a government website protection system

- Development of a monitoring and evaluation program for the level of Greek cyberspace security (threat intelligence tool)

- Installation and configuration of an open-source automated alert system tool regarding the availability of websites and network devices

- Installation of an open-source platform for vulnerability assessment and performance of Penetration tests

- Installation and configuration of open-source tool for exchange of IOCs indicators with other cybersecurity organizations (**National CERT, CERT/Cyber Defence Directorate, CERT GRnet, 4thCERT**)

9.2 SPECIFIC OBJECTIVE 3.B.: STRENGTHEN DETERRENCE MECHANISMS AND ENHANCE OPERATIONAL COOPERATION

Fighting against cybercrime requires appropriate tools at the disposal of the competent Entities, as it consists one of the threat factors that may have a large impact on the services provided by the Entities. It is therefore necessary to strengthen the legal framework and the competent services that will oversee its suppression. In particular, in the context of this objective, a cooperation framework (holding meetings, assessing the level of compliance with existing provisions, parameters and evolution of cybercrime in the country, at international and European level) between the relevant Services (e.g. Cybercrime Division, Ministry of Justice, Ministry of Foreign Affairs) plays a key role. Furthermore, an important action is the mapping of the existing institutional framework and sanctioning provisions, as a basis for evaluating the progress of its implementation, including the level of deterrence, but also the implementation of interventions to strengthen the sanctioning framework in cooperation with the relevant entities.

9.3 SPECIFIC OBJECTIVE 3.C.: CYBERSECURITY FOR THE PROTECTION OF PRIVACY

The Strategy is in line with the requirements of the regulations and current legislation for the protection of such data, through, inter alia, the integration of data protection principles (data protection by design) in the basic requirements and principles of cybersecurity and cooperation with competent bodies (e.g. Hellenic Data Protection Authority -HDPA). A key action in this regard is the coordination of incident reporting procedures with stakeholders, through the development of institutional cooperation / joint cooperation group with HDPA and Hellenic Authority for Communication Security and Privacy in the context of privacy protection. At the same time, an important framework for intervention is the collection, analysis and documentation of cyber-attack data involving invasion of privacy, in order to obtain a comprehensive picture of these incidents, as well as to take further action to address them.

Objectives	Activities	Milestones
3.A. Optimise methods, techniques and tools utilised in incident analysis, response and reporting	**3.A.1.** Establishment of a Critical Infrastructure Monitoring Security Operations Centre - SOC	Q4 2022 - Continuous activity
	3.A.2. Creation of a Cyber hotline	Q2 2023 - Continuous activity
	3.A.3. Definition of an incident management framework	Q2 2022
	3.A.4. Establishment and management of an event log (formal and / or anonymous), including all information related to the event, actions taken, results, lessons learned.	Q4 2023 - Continuous activity
	3.A.5. Operation of a government website protection system	Q4 2021 - Continuous activity
	3.A.6. Development of reek cyberspace security monitoring and evaluation platform (threat intelligence tool)	Q1 2022 - Continuous activity
	3.A.7. Installation and configuration of open-source tool for automatic notification regarding websites and web devices availability	Q4 2022 - Continuous activity
	3.A.8. Installation of open-source platform for vulnerability assessment and Penetration tests	Q4 2022 – continuous activity
	3.A.9. Installation and configuration of a log file & malware analysis tool	Q4 2022 - Continuous activit
	3.A.10. Installation and configuration of an open source tool for exchanging IOCs with other cybersecurity organizations (National CERT, CERT/ ΔΙΚΥΒ, CERT GRnet, FORTHcert)	Q4 2023 - Continuous activit
	3.A.11. Establishment of a central reporting mechanism under GDPR, NISD, art. 13a, eIDAS	Q2 2023 - Continuous activit
	3.A.12. Preparation of annual bulletins and landscape reports on cyber-attacks incidents	Q4 2O24 - Continuous activit
	3.A.13. Establismento of a log files and cyber incidents analysis lab (forensics lab)	Q4 2O24 - Continuous activit

9.4 FLAGSHIP ACTIVITIES

Objectives	Activities	Milestones
3.B. Strengthen deterrence mechanisms and enhance operational cooperation	**3.B.1.** Development of a network of enhanced cooperation in the fight against cybercrime	Q4 2021 - Continuous activity
	3.B.2. Elaboration of a comprehensive proposal for the sanctions' framework of public cybersecurity policy	Q2 2024
	3.B.3. Development and utilization of modern tools and techniques for the fight against cybercrime	Q1 2021 - Q4 2025
3.C. Cybersecurity for the protection of privacy	**3.C.1.** Development of institutional cooperation / joint cooperation group with HDPA and ADAE in the context of privacy protection	Q4 2021 - Continuous activity
	3.C.2. Development and monitoring of a data recording platform regarding cyber-attack data that involve privacy breaches	Q2 2024

10 STRATEGIC GOAL 4: A MODERN ENVIRONMENT FOR CYBERSECURITY INVESTMENTS WITH EMPHASIS ON THE PROMOTION OF RESEARCH AND DEVELOPMENT

10.1 SPECIFIC OBJECTIVE 4.A.: ENCOURAGE R&D INITIATIVES

One of the most important areas for strengthening the national level of cybersecurity is state support for research and development both at the academic and private level. These initiatives may involve the participation of Institutions (public and / or private) in European competitions aimed at developing critical new technologies and cybersecurity measures, or strengthening the actions of private Institutions in the field of applied research, or even the reform of curricula to cover cybersecurity issues (eg enhancing postgraduate programs, seminars, certifications, etc.).

The Authority will be the contact point between all Stakeholders, so that, taking into account the relevant information and having an in-depth understanding of the ever-changing ICT environment, it will provide guidelines for targeted actions with clear timelines and expected results. In particular, in the context of this objective, individual actions are:

Figure 15 *Promote Research and Development (R&D) in the cybersecurity sector*

The above interventions will be systematized in the context of the preparation of a medium-term R&D agenda with topics that promote the implementation of the cybersecurity strategy and networking for the development of innovations in the field of cyber security (eg technology parks, innovation complexes, etc.). In this light, a key factor is the development of enhanced collaboration with academic and research institutions.

10.2 SPECIFIC OBJECTIVE 4.B.: PROVIDE INVESTMENT INCENTIVES

The successful implementation of the Strategy is based on the investment of the Entities in organizational, technical and other cyber security measures. As a direct consequence of cyber security risk assessment, Entities should implement the necessary measures to ensure their (business) operations in accordance with the basic requirements and principles of cyber security. The Strategy sets incentives for the Entities to mobilize them to implement appropriate actions, thus strengthening their profile and contributing to the successful response to incidents. In this light, key actions constitute:

- Available financial resources mapping and strengthening their utilization system
- Providing targeted incentives (e.g. tax/fiscal, financial, etc)
- Innovative tools development for strengthening entities' cyber security

For the effective financing of these interventions, the creation of an incentive toolkit in cooperation with the competent bodies on a case-by-case basis is preferred, with the aim of motivating companies to invest in cyber security measures. This toolkit may include fiscal and financial incentives, such as reduced taxation, subsidy, etc. Furthermore, the development and

utilization of innovative financing mechanisms as well as mechanisms for optimization - acceleration and simplification of procedures for the financing of cybersecurity actions, will make a key contribution to the fight against bureaucracy and the more efficient allocation of resources for the benefit of the Entities.

10.3 SPECIFIC OBJECTIVE 4.C: UTILISE PPPS

Sound cooperation between the Public and Private sectors is a critical factor in the success of the National Cybersecurity Strategy, as accredited companies will be able to provide, at their disposal, services through Public-Private Partnerships (PPPs). In this context, a critical action is the compilation of a registry of private entities, which, if they meet specific conditions (accreditation) will partner with public entities, in order to provide specialized services for the benefit of digital governance. For example:

- Security consulting services
- Interconnection and protection services against DoS / DDoS attacks
- Technical inspection security services
- Threat intelligence services
- Installation and operation of equipment and / or security software

The registry may contain information such as:

- Matching entities with services that may be requested by the Authority, either for internal purposes or on behalf of the supervised entities
- Cost indication per executive level
- Procedure for the issue of work orders or mini-tenders for specific items
- Service providers / Services response level (SLA)
- Indicative terms of transactions, invoicing, clauses, etc.

Furthermore, it is proposed to accredit these entities, through criteria concerning indicatively:

- The provider ‘s and its executives experience
- Certifications
- Presence in the Greek market
- Projects in European organizations

10.4 FLAGSHIP ACTIVITIES

Objectives	Activities	Milestones
4.A. Encourage R&D initiatives	**4.A.1.** Preparation of a medium-term R&D agenda with topics that promote the implementation of the cybersecurity strategy	Q1 2022 - Continuous activity
	4.A.2. Promotion of networking for the implementation of innovations in the field of cybersecurity (technology parks, innovation complexes etc.)	Q2 2023 - Continuous activity
	4.A.3. Development of enhanced cooperation with academic and research institutions in cybersecurity issues	Q2 2022 - Continuous activity
4.B. Provide investment incentives	**4.B.1.** Creation of a toolkit to motivate companies to invest in cybersecurity measures using fiscal and financial incentives such as. reduced taxation, grants, etc.	Q2 2022 - Continuous activity
	4.B.2. Development of innovative financing mechanisms	Q2 2022 - Continuous activity
4.C. Utilise PPPs	**4.C.1.** Definition of requirements for providers 0f cybersecurity services	Q3 2022
	4.C.2. Establishment of a program partnership with the PPPs Special Secretariat	Q4 2021
	4.C.3. Establishment of a partner companies registry	Q4 2022

11 STRATEGIC GOAL 5. CAPACITY BUILDING, PROMOTING INFORMATION AND AWARENESS RAISING

11.1 SPECIFIC OBJECTIVE 5.A.: BUILDING CAPACITY BY ORGANISING CYBERSECURITY EXERCISING ACTIVITIES

A main goal of the Strategy is to create a framework for ongoing training and readiness assessment of the Entities to respond to cyber security incidents. To this end, the Authority, in cooperation with National and European bodies, will determine the content and pace of cyber security exercises, in order to identify, as far as possible, threats that may affect the functions of the Public Administration and the other Stakeholders. The National Readiness Exercises are an important tool for assessing the readiness of the participating entities and identifying the weaknesses and vulnerabilities of the systems. The security incident simulation enables security incidents to be dealt as real-world situations, by implementing established security measures and contingency plans, so that Entities can make relevant improvements and updates. Furthermore, these exercises strengthen the exchange of information and knowledge, the cooperation between the participating entities and, at the same time, the cooperation culture for the increase of Cyber Security level in the country.

Readiness exercises are conducted at regular intervals. The exercises are supervised by the National Cybersecurity Authority and are planned based on clearly defined schedules, roles, scenarios and objectives. The results of the exercises and especially the knowledge acquired must be communicated to those involved in the exercises, but also to other competent bodies. Greece seeks to participate in European and international preparedness exercises. For the implementation of the exercises, specific online platforms can be used that provide functionalities for defining scenarios, defining teams (attackers, defenders), monitoring the progress of the exercise, recording skills per group and its member, as well as collaborating with a variety of organizations from critical sectors. At the same time, the Authority will actively participate in exercises such as Cyber Europe organized by the European Information and Network Security Organization (ENISA) or Locked Shields organized by NATO or PANOPTIS organized by the Greek state.

11.1.1 Development and use of "cyber range" type platform

As cybersecurity exercises at national level are difficult to organize, and require significant funding for their planning and successful completion, the Authority is proposed to develop or use a cyber range platform. These online platforms aim to create an environment that simulates real networks, attackers and users, through a simulation framework that is found in online games. Essentially, cyber range platforms are used as follows:

- The exercise leader (e.g. the National Cybersecurity Authority) defines the environment for which an exercise will take place, while grouping users (e.g. Entities executives) into a red team (attackers) and a blue team (defenders). At the same time, it sets goals and the time frame within which the exercise should be completed

- Each team has a scenario to follow, with a variety of tools available, such as penetration testing tools, forensic tools, etc.

- The leader knows the solution for each possible scenario, per group, and can provide brief information (tips) to its members, which may, however, consume points (if specified by the leader) in order to gain access to part of the solution. exercise. The lower the points of a team, the lower its "rating" against the "opponent"

- The leader monitors the progress of the team members and is able to understand any gaps that exist regarding skills, response times, etc., in order to produce the appropriate reports that will be used for further training of other Entities members

- Team members collaborate, exchange ideas, try new practices and tools while understanding their skill level in a variety of scenarios that are potentially real threat scenarios

- Therefore, the development or use of an existing platform (by specialized providers), will help to create the appropriate environment for the technical training of the Entities executives, maintaining their constant vigilance against cyber threats that may jeopardize their operation and services providing

11.2 SPECIFIC OBJECTIVE 5.B.: APPLY STATE - OF - THE - ART EDUCATIONAL AND TRAINING METHODS AND TOOLS

Particular emphasis is placed on the preparation of future executives of the Entities in the field of cybersecurity, for which practical support is required from higher education institutions. Inextricably linked to the strengthening of research and development and the cooperation between Entities, is to create appropriate incentives for the younger generations to come in direct contact with cybersecurity and to be able to choose it as a subject of study or specialization. The ultimate goal is to establish a cyber-hygiene framework and to create a positive culture towards cybersecurity.

In particular, among the flagship activities of this specific objective are:

11.2.1 Education and Awareness Action Plan

Capacity building, systematic and ongoing training, as well as raising awareness and maintaining a high level of awareness of all participants in the National Cybersecurity Ecosystem, are key elements in ensuring vigilance against threats and effective response to security incidents.

Crucial for the successful outcome of the actions of this strategic goal, is the development of an education plan compatible and harmonized with the needs of the Ecosystem. The plan should set specific goals for educating and informing the various stakeholders and outline the roadmap for achieving them.

An **Education and Awareness Action Plan** should include an analysis of the current situation (long established actions and stakeholders, cybersecurity culture, the role of academic institutions, etc.), in order to highlight ecosystem deficiencies. The plan must be complemented by targeted actions and activities. It is necessary to distinguish the relevant activities, depending on the audience to which they are addressed (cybersecurity professionals, business executives, citizens, etc.).

The Education and Awareness Action Plan accompanies the other specific objectives, providing guidelines for improving the culture, perception but also the required know-how for a high level information security. It must also be supported by mechanisms to monitor and measure the achievement of the relevant objectives.

11.2.2 Framework for upgrading Expertise and Skills of Professionals

A main goal of the Strategy is to create a framework for continuous training and readiness of the Entities to respond to cyber security incidents. To this end, the competent entities must define specific actions and interventions, which relate to the following pillars.

- Academic Education

  Particular emphasis is placed on the preparation of the Entities future executives in the field of cybersecurity, for which the academic institutions play a key role, by creating both appropriate undergraduate and postgraduate study programs, and appropriate incentives for students to attend relevant fields of study.

  Relevant actions are: a) the assessment of the coverage of the minimum competencies required by the existing threat landscape and b) the definition of targeted actions to attract students.

- Professional Training

  Equally important is the regular update of the knowledge and skills of

professionals, as technological developments and threats are constantly changing.

Relevant actions are: a) the definition of incentives for public and private enterprises and their professionals, for the participation of the latter in training actions and b) the development of specialized training programs.

- Lifelong Learning

  Curricula that support professionals in relevant professions and professional disciplines, in order to be informed and trained in appropriate areas of cybersecurity, thus enriching the available human resources.

  Relevant actions are: a) the recording and analysis of the existing lifelong learning framework and b) the development of proposals for interventions related to attracting professionals from different fields.

Especially for actions related to academic education, it is advisable to design professional profiles for the various roles in the field of cybersecurity. The clear definition of roles includes a description of qualifications, tasks, which assist in any training and education action. It also provides clear vocational guidance to young people interested in this field.

Especially for capacity building actions, a particularly effective mechanism is to conduct cyber security exercises, which simulate security incidents based on predefined scenarios. These exercises serve the participants in many ways: a) assessment of preparedness and contingency plans, b) cultivating information and knowledge exchange and cooperation, c) testing and developing skills.

11.2.3 Creating material

Having understood and defined the target groups that each educational action will have set as a goal, the Authority is proposed to proceed with the appropriate material development. The need for participation of other authorities, such as ENISA, HDPA, EETT, the Greek Police Cybercrime Division, private bodies, etc. is emphasized.

The material concerns, among others:

- Information for executives - presentation: It will provide to the executives of the Entities the basic principles of the new culture, the new desired behaviours as well as issues that may arise for the respective Entity from the non-application of the new rules and procedures by the employees. This presentation can be used during the recruitment of new executives

- Information material - brochures and posters: For topics such as: Malware, Social engineering and phishing, Personal data protection,

study visits, Mobile devices, Use of e-mail, Website visits, Protection of equipment during the holidays, etc.

- Informative emails / emails with tips: They will be sent to the executives in specific time periods where the frequency of incidents for data leaks or thefts is higher and will include warnings regarding viruses or other dangers (e.g. October - cyber security, November Black Friday, Christmas-New Year period, discount periods, Easter, summer holidays, long weekends)

- E-learning programs: They will include a test in which Executives will be asked to confirm that they understand the rules and behaviours imposed by the new information security culture. The program will cover the following indicative topics: Entity s Data Protection, personal data protection, System Usage Proper Use, Security passwords proper Use, Corporate Email Proper Usage, Mobile Devices and Storage Units, Social Engineering, Security Incident Reporting, Best Practices, Physical security, etc.

- Educational program for Informatics Department/Division staff (system administrators, developers, etc.)

- Training of trainers - executives of the Entities who will then undertake the implementation of trainings in matters of data management & data protection

- Frequently asked questions (FAQ): Identify possible questions and related answers (can be posted on websites, etc.)

- Hotline where Entities (OES and DSPs) will be able to address for clarifications, questions or other issues related to information security (process, questions, escalation points, role description, etc.)

- Online alerting application: Installation and use of a digital application tool that aims to enhance the educational messages to users, reminding them via mobile messages of the importance of security and data protection, thus helping to establish the desired behaviours

11.2.4 Seminars

Special emphasis will be given to training seminars for Security and Networks Officers which will be organized by the Authority.

11.3 SPECIFIC OBJECTIVE 5.C.: PROMOTE OPEN - ENDED CYBERSECURITY INFORMATION AND AWARENESS RAISING FOR ENTITIES AND CITIZENS

The successful implementation of the National Cybersecurity Strategy also depends on the promotion of a security culture at national level. Constantly informing the general population is one of the most critical success factors of the Strategy, and therefore the existing awareness and information actions (as a result of the Education and Awareness Action Plan) should be evaluated and the areas needing further action should be defined.

In cooperation with the competent national organizations, it is proposed to create a **National Cyber Security Awareness Program**, in order to fully cover all age and social groups of citizens, with appropriate and up-to-date information material. The ultimate goal is to establish a cyber-hygiene framework and a cyber security awareness national culture.

11.4 FLAGSHIP ACTIVITIES

Objectives	Activities	Milestones
5.A. Building capacity by organising cybersecurity excercising activities	**5.A.1.** Elaboration of the National Program for Cyber Security Exercises	Q1 2022 - Continuous activity
	5.A.2. Capacity building and “lessons learnt” procedures	Q1 2022 - Continuous activity
	5.A.3. Utilization of a “cyber range” type platform for the training of managers (security, networks, systems, applications, databases, etc.) of the Authority and the Entities	Q1 2022 - Continuous activity
5.B. Apply state - of - the - art educational and training methods and tools	**5.B.1.** Information and educational material compilation (general and by Entities category)	Continuous activity
	5.B.2. Elaboration of an Education and Awareness Action Plan	Q1 2022
	5.B.3. Framework for upgrading Expertise and Skills of Professionals	Q4 2024 - Continuous Activity
5.C. Promote open - ended cybersecurity information and awareness raising for Entities and citizens	**5.C.1.** Elaboration of the National Program for Cybersecurity Awareness	Q4 2023 - Continuous activity
	5.C.2. Configuration of an incident communication management framework	Q1 2022 - Continuous activity

12 EVALUATION AND FEEDBACK

The implementation of the strategic goals of the National Cybersecurity Strategy is monitored by the National Cybersecurity Authority, in order to evaluate and initiate feedback to the Strategy. In particular, with regard to the evaluation and feedback process of the Strategy, an integrated system will be put in place to monitor and evaluate the implementation of the Strategy through the development of appropriate measurement indicators (KPIs, KRIs), issuance of periodic reports and annual report of actions and results (along with threat landscape report), but also utilization of tools and best practices (e.g. ENISA):

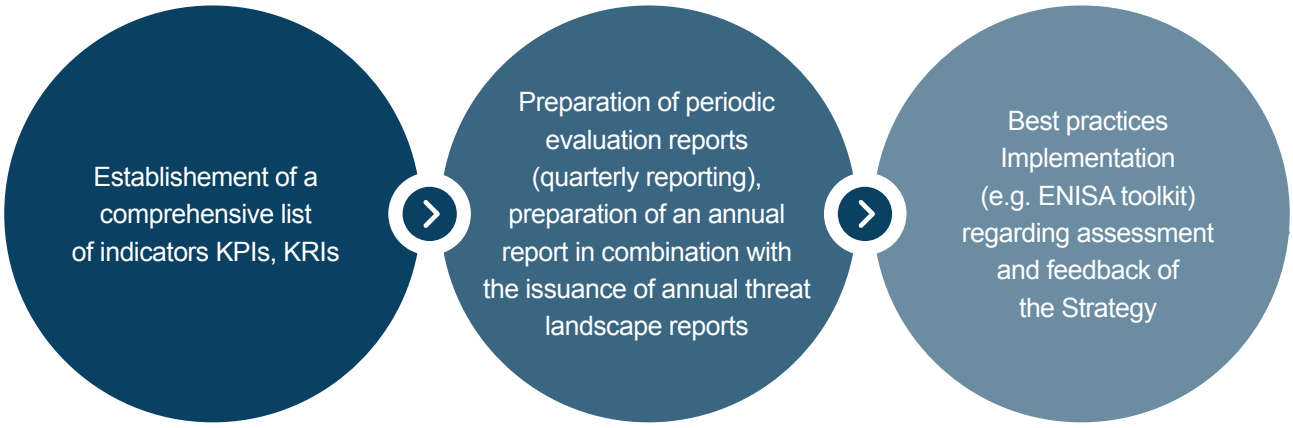

Figure 16 *Evaluation and feedback framework of the National Cybersecurity Strategy*

Taking into account the need to shape a longer-term horizon in the implementation of the described initiatives and actions, the preferred option is to update this strategy every five years.

13
TABLE OF FLAGSHIP ACTIVITIES

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
1. A functional cybersecurity governance system	**1.A.** Optimize Organisational structures and Procedures	**1.A.1.** Development of an integrated cybersecurity management system for public sector entities	National Cybersecurity Authority, central government entities, National CERT, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE	**1.A.1.K.1.** Number of CISO /Number of Central Government Entities **1.A.1.K.2.** Number of Bodies evaluated	Q2 2021
		1.A.2. Development of a framework for the promotion of cybersecurity excellence management	National Cybersecurity Authority	**1.A.2.K.1.** Number of Bodies certified **1.A.2.K.2.** Determination of a comprehensive performance indicator	Q3 2022 - Continuous activity
		1.A.3. Drafting of sectoral action plans (e.g. Energy, Healthcare, Transport, Finance, Telco, Maritime, etc.)	National Cybersecurity Authority sectoral ministries, OES, DSP, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE, National CERT	**1.A.3.K.1.** Number of projects drawn up / Number of sectors	Q4 2024
		1.A.4. Reinforcement of information sharing mechanisms	National Cybersecurity Authority, All parties concerned	**1.A.4.K.1.** Number of sharing information network operators	Q2 2022

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
1. A functional cybersecurity governance system	**1.B.** Apply vigorous risk assessment and effective contigency planning	**1.B.1.** Development of a data analysis methodology and a threat Registry	National Cybersecurity Authority, central government entities, OES/ DSP, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE, National CERT, Centre for Security Studies	**1.B.1.K.1.** System data set	Q4 2021
		1.B.2. National risk assessment planning	National Cybersecurity Authority, central government entities, OES/ DSP, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE, Centre for Security Studies	**1.B.2.K.1.** Planning completion	Q4 2021 - Continuous assessment and updating
		1.B.3. National contingency planning	National Cybersecurity Authority, central government entities, OES/ DSP, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE, National CERT, Centre for Security Studies	**1.B.3.K.1.** Planning completion	Q4 2021 - Continuous assessment and updating

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
1. A functional cybersecurity governance system	**1.C.** Strengthen national, European and international collaborations	**1.C.1.** Strengthening the Greek presence and participation in international alliances on cybersecurity issues	National Cybersecurity Authority, MFA, National CERT	**1.C.1.K.1.** Number of collaborations/ alliances	Continuous activity
		1.C.2. Support for cooperation with third countries in the bilateral transfer of know-how with the aim of strengthening the common high level of security and efficiently responding to cross-border threats	National Cybersecurity Authority, MFA, National CERT	**1.C.2.K.1.** Number of collaborations **1.C.2.K.2.** Number of relevant actions	Continuous activity
		1.C.3. Establish a methodology for international collaborations on cybersecurity issues and conclude cooperation agreements with third countries	National Cybersecurity Authority, MFA, National CERT	**1.C.3.K.1.** Number of cooperation pacts	Q4 2021 - Continuous activity
		1.C.4. Creation of a management model to facilitate progress in cooperation initiatives in order to enhance the national level of security, develop skills and build awareness through cooperation	National Cybersecurity Authority, MFA, National CERT	**1.C.4.K.1.** International indicators ranking	Q4 2021 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
2. Shielding Critical Infrastructures and securing new technologies	**2.A.** Comprehend technological developments and their effects on digital governance	**2.A.1.** Implementation of an integrated cybersecurity framework for 5G networks	National Cybersecurity Authority, Hellenic Authority for Communication Security and Privacy, Hellenic Telecommunications and Post Commission, MFA, National CERT	**2.A.1.K.1.** Establishing a framework	Q4 2021 - Continuous activity
		2.A.2. Implementation of a framework of security measures and actions for Artificial Intelligence	National Cybersecurity Authority, National CERT	**2.A.2.K.1.** Framework adoption/issuance	Q4 2021 - Continuous activity
		2.A.3. Implementation of a framework of security measures and actions for the Internet of Things (IoT)	National Cybersecurity Authority, National CERT	**2.A.3.K.1.** Framework adoption/issuance	Q4 2021 - Continuous activity
		2.A.4. Development of enhanced collaboration with academic and research institutions on new technologies	National Cybersecurity Authority, scientific - research bodies, GSRT, National CERT	**2.A.4.K.1.** Number of collaborations implemented	Q4 2021 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
2. Shielding Critical Infrastructures and securing new technologies	**2.B.** Upgrade critical infrastructures protection	**2.B.1.** Defining and updating a list of critical infrastructures	National Cybersecurity Authority	**2.B.1.K.1.** Catalogue release	Q4 2022
		2.B.2. Development and implementation of a coordination framework for CISOs	National Cybersecurity Authority, OES / DSP	**2.B.2.K.1.** Framework adoption	Q1 2022
		2.B.3. Development of practices for detection, quantification, prioritization, early warning and risk management for critical infrastructure	National Cybersecurity Authority, OES / DSP, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE, National CERT	**2.B.3.K.1.** Risk assessment Issuance	Q4 2022
		2.B.4. Preparation of threat landscape reports	National Cybersecurity Authority, Central Government Entities, OES/ DSP, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE, National CERT, Centre for Security Studies	**2.B.4.K.1.** Number of reports / year	Q4 2025

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
2. Shielding Critical Infrastructures and securing new technologies	**2.C.** Consolidate systems and applications by implementing enhanced security requirements	**2.C.1.** Development and management of a hardware, software and intangible information assets registry in critical sectors (public, critical infrastructure)	National Cybersecurity Authority	**2.C.1.K.1.** Number of infrastructures register	Q4 2021 - Continuous activity
		2.C.2. Categorization of entities for the determination of enhanced security requirements	National Cybersecurity Authority	**2.C.2.K.1.** Number of classified bodies / entities	Q2 2023
		2.C.3. Issuance of enhanced security requirements (horizontal and sectoral) taking into account international and European standards and certification frameworks	National Cybersecurity Authority, central government bodies OES/ DSP, CSIRT HNDGS / CYBER DEFENCE DIRECTORATE, National CERT, Centre for Security Studies	**2.C.3.K.1.** Security requirements issuance	Continuous activity
		2.C.4. Issuance of special security requirements for public ICT projects	National Cybersecurity Authority	**2.C.4.K.1.** Specific requirements issuance	Q4 2022 - Continuous activity
		2.C.5. Development of an audit system for the implementation of security requirements	National Cybersecurity Authority	**2.C.5.K.1.** Audits/year **2.C.5.K.2.** Bodies audited / year	Q4 2021 - Continuous activity
		2.C.6. Development of an integrated system for assessing the maturity level of entities	National Cybersecurity Authority	**2.C.6.K.1.** Bodies evaluated	Q4 2021 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
3. Incident management optimisation, fight against cybercrime and privacy protection	**3.A.** Optimise methods, techniques and tools utilised in incident analysis, response and reporting	**3.A.1.** Establishment of a Critical Infrastructure Monitoring Security Operations Centre - SOC	National Cybersecurity Authority, National CERT	**3.A.1.K.1.** Number of incidents management / year	Q4 2022 - Continuous activity
		3.A.2. Creation of a Cyber hotline	National Cybersecurity Authority, National CERT	**3.A.2.K.1.** Number of calls	Q2 2023 - Continuous activity
		3.A.3. Definition of an incident management framework	National Cybersecurity Authority, National CERT, CSIRT, HNDGS /CYBER DEFENCE DIRECTORATE, Centre for Security Studies, HACSP, HDPA	**3.A.3.K.1.** Framework adoption	Q2 2022
		3.A.4. Establishment and management of an event log (formal and / or anonymous), including all information related to the event, actions taken, results, lessons learned	National Cybersecurity Authority, National CERT, CSIRT, HNDGS /CYBER DEFENCE DIRECTORATE, Centre for Security Studies, HACSP, HDPA	**3.A.4.K.1.** Incidents and data entered in the register/month	Q4 2023 - Continuous activity
		3.A.5. Operation of a government website protection system	National Cybersecurity Authority, National CERT	**3.A.5.K.1.** Number of websites protected	Q4 2021 - Continuous activity
		3.A.6. Development of reek cyberspace security monitoring and evaluation platform (threat intelligence tool)	National Cybersecurity Authority, National CERT	**3.A.6.K.1.** System implementation **3.A.6.K.2.** Set of threads recorded **3.A.6.K.3.** Number of bodies / devices integrated	Q1 2022 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
3. Incident management optimisation, fight against cybercrime and privacy protection	**3.A.** Optimise methods, techniques and tools utilised in incident analysis, response and reporting	**3.A.7.** Installation and configuration of open-source tool for automatic notification regarding websites and web devices availability	National Cybersecurity Authority, National CERT	**3.A.7.K.1.** System implementation **3.A.7.K.2.** Set of threads recorded **3.A.7.K.3.** Number of bodies / devices integrated	Q4 2022 - Continuous activity
		3.A.8. Installation of open-source platform for vulnerability assessment and Penetration tests	National Cybersecurity Authority, National CERT	**3.A.8.K.1.** System implementation **3.A.8.K.2.** Set of threads recorded **3.A.8.K.3.** Number of bodies / devices integrated	Q4 2022 - Continuous activity
		3.A.9. Installation and configuration of a log file & malware analysis tool	National Cybersecurity Authority, National CERT	**3.A.9.K.1.** System implementation **3.A.9.K.2.** Set of threads recorded **3.A.9.K.3.** Number of bodies / devices integrated	Q4 2022 - Continuous activity
		3.A.10. Installation and configuration of an open source tool for exchanging IOCs with other cybersecurity organizations (National CERT, CERT / ΔΙΚΥΒ, CERT GRnet, FORTHcert)	National Cybersecurity Authority, National CERT, CERT / CYBER DEFENCE DIRECTORATE, CERT GRnet, FORTHCERT	**3.A.10.K.1.** Set of indicators exchanged / month	Q4 2023 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
3. Incident management optimisation, fight against cybercrime and privacy protection	**3.A.** Optimise methods, techniques and tools utilised in incident analysis, response and reporting	**3.A.11.** Establishment of a central reporting mechanism under GDPR, NISD, art. 13a, eIDAS	National Cybersecurity Authority, National CERT, CSIRT, HNDGS /CYBER DEFENCE DIRECTORATE, Centre for Security Studies, HACSP, HDPA	**3.A.11.K.1.** Set of incidents included in the mechanism/year	Q2 2023 - Continuous activity
		3.A.12. Preparation of annual bulletins and landscape reports on cyber-attacks incidents	National Cybersecurity Authority, National CERT, CSIRT, HNDGS / CYBER DEFENCE DIRECTORATE, Centre for Security Studies	**3.A.12.K.1.** Set of reports/ year	Q4 2024 - Continuous activity
		3.A.13. Establismento of a log files and cyber incidents analysis lab (forensics lab)	National Cybersecurity Authority, National CERT	**3.A.13.K.1.** Laboratory implementation	Q4 2024 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
3. Incident management optimisation, fight against cybercrime and privacy protection	**3.B.** Strengthen deterrence mechanisms and enhance operational cooperation	**3.B.1.** Development of a network of enhanced cooperation in the fight against cybercrime	National Cybersecurity Authority, Ministry of Justice, Cyber Crime Division, Ministry of Foreign Affairs	**3.B.1.K.1.** Meetings / month	Q4 2021 - Continuous activity
		3.B.2. Elaboration of a comprehensive proposal for the sanctions' framework of public cybersecurity policy	National Cybersecurity Authority	**3.B.2.K.1.** Set of infringements / year	Q2 2024
		3.B.3. Development and utilization of modern tools and techniques for the fight against cybercrime	National Cybersecurity Authority, Ministry of Justice, Cyber Crime Division, Ministry of Foreign Affairs	**3.B.3.K.1.** Set of infringements / year	Q1 2021 - Q4 2025
	3.C. Cybersecurity for the protection of privacy	**3.C.1.** Development of institutional cooperation / joint cooperation group with HDPA and ADAE in the context of privacy protection	National Cybersecurity Authority, Hellenic Authority for Communication Security and Privacy, HDPA	**3.C.1.K.1.** Group meetings per year	Q4 2021 - Continuous activity
		3.C.2. Development and monitoring of a data recording platform regarding cyber-attack data that involve privacy breaches	National Cybersecurity Authority, Hellenic Authority for Communication Security and Privacy, HDPA	**3.C.2.K.1.** Data logged on the platform	Q2 2024

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
4. A modern environment for cybersecurity investments with emphasis on the promotion of Research and Development	**4.A.** Encourage R&D initiatives	**4.A.1.** Preparation of a medium-term R&D agenda with topics that promote the implementation of the cybersecurity strategy	National Cybersecurity Authority, Ministry of Education, Ministry of Development and Investment, scientific and research bodies, KETYAK / NIS	**4.A.1.K.1.** Issue an agenda	Q1 2022 - Continuous activity
		4.A.2. Promotion of networking for the implementation of innovations in the field of cybersecurity (technology parks, innovation complexes etc.)	National Cybersecurity Authority, Ministry of Education, Ministry of Development and Investment, scientific and research bodies, KETYAK / NIS	**4.A.2.K.1.** Number of technology parks, innovation clusters etc.	Q2 2023 - Continuous activity
		4.A.3. Development of enhanced cooperation with academic and research institutions in cybersecurity issues	National Cybersecurity Authority, Ministry of Education, Ministry of Development and Investment, scientific and research bodies, KETYAK / NIS	**4.A.3.K.1.** Cooperations/ year	Q2 2022 - Continuous activity
	4.B. Provide investment incentives	**4.B.1.** Creation of a toolkit to motivate companies to invest in cybersecurity measures using fiscal and financial incentives such as. reduced taxation, grants, etc.	National Cybersecurity Authority, Ministry of Development and Investment, Ministry of Finance	**4.B.1.K.1.** Number of bodies who received funding	Q2 2022 - Continuous activity
		4.B.2. Development of innovative financing mechanisms	National Cybersecurity Authority, scientific -research bodies, GSRT	**4.B.2.K.1.** Number of bodies who received funding	Q2 2022 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
4. A modern environment for cybersecurity investments with emphasis on the promotion of Research and Development	**4.C.** Utilise PPPs	**4.C.1.** Definition of requirements for providers 0f cybersecurity services	National Cybersecurity Authority, Ministry of Development and Investment, Ministry of Finance	**4.C.1.K.1.** Issue requirements	Q3 2022
		4.C.2. Establishment of a program partnership with the PPPs Special Secretariat	National Cybersecurity Authority, Ministry of Development and Investment, Ministry of Finance	**4.C.2.K.1.** Meetings/Year	Q4 2021
		4.C.3. Establishment of a partner companies registry	National Cybersecurity Authority, Ministry of Development and Investment, Ministry of Finance	**4.C.3.K.1.** Companies entered in register	Q4 2022

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
5. Capacity building, promoting information and awareness raising	**5.A.** Building capacity by organising cybersecurity excersising activities	**5.A.1.** Developing a comprehensive program of exercises implementation	National Cybersecurity Authority, involved Bodies where appropriate	**5.A.1.K.1.** Set of exercises/year **5.A.1.K.2.** Total number of trainees/year	Q1 2022 - Continuous activity
		5.A.2. "Lessons learnt" capacity and procedures building	National Cybersecurity Authority	**5.A.2.K.1.** Set of records in the exercise repository	Q1 2022 - Continuous activity
		5.A.3. Using a "cyber range" type platform for the training of the Authority and Bodies managers (security, networks, systems, applications, databases etc.)	National Cybersecurity Authority	**5.A.3.K.1.** Set of exercises/year **5.A.3.K.2.** Total number of trainees/year	Q1 2022 - Continuous activity
	5.B. Apply state - of - the - art educational and training methods and tools	**5.B.1.** Information and educational material compilation (general and by Entities category)	National Cybersecurity Authority, education providers	**5.B.1.K.1.** Number of material distributed	Continuous activity
		5.B.2. Elaboration of an Education and Awareness Action Plan	National Cybersecurity Authority	**5.B.2.K.1.** Elaboration of an Action Plan	Q1 2022
		5.B.3. Framework for upgrading Expertise and Skills of Professionals	National Cybersecurity Authority, education providers	**5.B.3.K.1.** Compilation of the study, publication **5.B.3.K.2.** Number of actions for attracting **5.B.3.K.3.** Number of participants	Q4 2024 - Continuous activity

Strategic Objectives	Specific Objectives	Flagship Activities	Bodies Involved /Stakeholders	KPIs	Milestones
5. Capacity building, promoting information and awareness raising	**5.C.** Promote open - ended cybersecurity information and awareness raising for Entities and citizens	**5.C.1.** Elaboration of the National Program for Cybersecurity Awareness	National Cybersecurity Authority, stakeholders' ecosystem	**5.C.1.K.1.** Number of actions **5.C.1.K.2.** Program implementation	Q4 2023 - Continuous activity
		5.C.2. Configuration of a communication incident management framework	National Cybersecurity Authority	**5.C.2.K.1.** Number of incidents managed in the communication field	Q1 2022 - Continuous activity


National Cyber Security Authority
HELLENIC REPUBLIC

HELLENIC REPUBLIC
MINISTRY OF DIGITAL GOVERNANCE
NATIONAL CYBERSECURITY AUTHORITY

DECEMBER 2020