DEPUTY MINISTRY OF RESEARCH, INNOVATION AND DIGITAL POLICY

DIGITAL SECURITY AUTHORITY

Policy paper

Cybersecurity Strategy of the Republic of Cyprus 2020

Security of Networks and Information and Protection of Critical Information Infrastructures

June 2020

TABLE OF CONTENTS

Executive Summary

Communication and information systems and technologies are today one of the most important factors in economic and social development, and undoubtedly constitute the necessary tools within the functional and social structures of each country. In parallel with the development of the cyberspace, the need to protect the electronic systems of organizations of all kinds is becoming more and more essential, so that any activity through these technologies is safe. A basic security system must cover the confidentiality, integrity and uninterrupted availability of the infrastructure and information, and must make the operation of the infrastructure reliable, flexible and controlled.

This Strategy aims to establish a secure electronic environment in the Republic of Cyprus, with special provisions and actions for the protection of critical Information infrastructures, where their disruption or destruction could have a serious impact on the vital social functions of the country. The elaboration of this Strategy has followed a holistic approach to responding to cyber threats, with the recognition that a proper strategy must contain multiple layers of security.

The main purpose of the Cybersecurity Strategy of the Republic of Cyprus is the protection of critical information infrastructures of the state and the operation of the country's communication and information technologies with the required levels of security, for the benefit of each user, the economy and the country. The implementation of the strategy's actions aims to make Cyprus one of the leading countries in the region in cybersecurity issues, in order to protect the critical information infrastructures of the state, businesses and society at large, and to create an appropriate and attractive environment for economic development and promotion of services in which Cyprus holds a high position worldwide such as, inter alia, merchant shipping and financial services.

This document revises and replaces the first Cybersecurity Strategy of the Republic of Cyprus and its main objective is to confront the threats that appear in cyberspace, at national level. Priority areas for achieving this objective that have been identified are as follows:

- the organization of the competent bodies of the State,
- the creation of an integrated legislative and regulatory framework,
- the creation or adaptation of the necessary structures and mechanisms within the Republic of Cyprus,
- the formulation of technical and organisational measures and procedures (in relation to the preparation, protection, detection and response to incidents),
- the development of the necessary competences and related training,
- the efficient cooperation of the state with competent bodies of the public and private sector,
- the development of research and innovation.

Therefore, this document contains a number of actions to achieve the above-mentioned objectives, in the following areas (thematic areas):

- Structures and Governance
- Institutionalisation of cooperation between competent public bodies
- Legal and Regulatory Framework
- National Government Security Framework
- Risk Assessment and Management – Criticality Assessment
- Incident Response and Crisis Management
- Capability Development – Organization and participation in Exercises
- Information Exchange – Situational Awareness
- Awareness – Creation of a Security Culture
- Education and training
- Research and innovation
- Cooperation with the private sector
- Security for All
- International Cooperation

In Annexes I, a summary of the actions is given for easy reference. For the preparation of the Strategy, in addition to national cybersecurity needs, the recommendations of the European Union Agency for Cybersecurity (ENISA), as well as the recommendations of other international bodies such as the International Telecommunication Union (ITU), have been taken into account. This Strategy also forms part and takes into account the broader National Security Strategy of the Republic of Cyprus.

1. INTRODUCTION

1.1. Cybersecurity Today

Communication and information systems and technologies are today one of the most important factors in economic and social development, and without a doubt constitute the necessary tools within the functional and social structures of each country. In parallel with the development of cyberspace, the need to protect the electronic systems of organizations of all kinds is becoming more and more essential, so that any activity through these technologies is safe. A basic security system must cover the confidentiality, integrity and uninterrupted availability of the infrastructure and information, and must make the operation of the infrastructure reliable, flexible and controlled.

The security of infrastructure refers to its ability and resilience to cope with risks and damage that may be caused to its various components. The security measures taken are mainly aimed at increasing preparedness and enhancing capabilities to prevent, detect and respond to potential risks, including malicious actions and/or attacks, and to take measures to mitigate and remedy any failures, malfunctions and availability of the services provided, including in emergency or crisis situations.

In this document, the terms ***'network and information security***' and ***'cybersecurity'*** are used. 'Network and information security' refers to the maintenance of confidentiality, integrity and availability as described below. 'Cybersecurity' refers to the broader security of networked systems operating in the cyberspace, mostly connected to the Internet, and this term includes the safe use of these systems by end-users.[1]

It is clarified that the level of information security must start from the determination of the ***value*** of information (and services), regardless of form (physical or electronic). This parameter will be taken into account in the implementation of the Actions of this document, and in particular those that have to do with informing the population for the purpose of cultivating awareness and a culture of security. As a more general principle, information in physical or electronic form should be adequately protected, depending on its value.

Network and information security is a key outcome of the development and dissemination of new communication and information technologies. In view of the globalisation of communications, especially with the use of the Internet as well as of the ever-increasing risks faced by users at all levels, it has become imperative to take measures for adequate protection and for the universal cooperation between all actors in society, public and private, at national, European and international level. Citizens, businesses and governments need to trust the means in which important information, personal and other data is handled.

The continuation of the secure development of communication and information technologies is important for citizens and societies, for the development of the labour sector and the economy in general, both at national, European and international level. Investment in security helps to increase users' confidence in new services and contributes to the wider development of the economy and society. Governments and businesses should evaluate investments in this sector on the basis of the cost they will have in the event of failure of their computer or communications systems due to malicious actions or natural causes.

Security in the world of information technology and electronic communications refers to ensuring three parameters:[2]

- **confidentiality** of information, i.e. allowing access to information only by authorised persons;
- **integrity of** the information, i.e. the protection of the information from any unwanted alteration or destruction,

[1] The standard ISO 27032 refers to the "preservation of the elements of confidentiality, integrity and availability of information in cyberspace and is based on information security, application security, network security and Internet security as fundamental building blocks.

[2] These parameters together compose the broader concept of ***resilience*** of the relevant infrastructure and systems.

- the **availability** of information or systems, i.e. allowing a system to provide the information when requested.

The assurance of the above parameters aims to maintain the security of networks and information to the greatest possible extent in relation to:

- Protection of information during transport (data in transit)
- Protection of information during **processing** (data in processing)
- Protection of information **during** storage (data in storage).

In addition to protecting infrastructure, systems and information, the maintenance of a high level of security based on the parameters mentioned above is essential for building **trust** in the information systems, communications and electronic services of the state and other important organizations in Cyprus. Building citizens' trust in these systems and ensuring secure cyber transactions will contribute significantly to the economic development of the country and to the fulfilment of the objectives of the Digital Agenda for Cyprus.

1.2. Critical Information Infrastructures

Information infrastructures in the Republic of Cyprus are now quite numerous and have penetrated almost every part of the life of average citizens. These infrastructures are used not only directly (e.g. by using telephone, Internet, etc.), as well as indirectly since almost all vital services in the country which are used by citizens are supported by information infrastructures. Some of these infrastructures form a vital part of the Cyprus economy and society, either by providing essential goods and services or by being the platform to support other (critical) infrastructures. They are thus considered *critical information* infrastructures, since their inactivation or destruction would have a serious impact on vital activities of society.

It is therefore necessary, through a broader framework of a state's cybersecurity strategy, to place particular emphasis on the protection of these critical information infrastructures. A number of actions described in this document cover the protection of critical information infrastructures, as well as the wider area of cybersecurity, as the two sectors are very closely linked and interact with each other. Section 3.5 "Risk Assessment and Management – Criticality Assessment", refers in greater detail to the procedure used to define the critical information infrastructures in the Republic of Cyprus.

1.3. Purpose

The purpose of the Cybersecurity Strategy of the Republic of Cyprus is the protection of the critical information infrastructures of the state and the operation of the country's communication and information technologies with the required levels of security, for the benefit of each user, the economy and the country.

1.4. Vision

Cyprus to become one of the leading countries in the region in cybersecurity issues, for the protection of critical information infrastructures of the state, businesses and society at large, and the creation of an appropriate and attractive environment for economic development and promotion of services in which Cyprus holds a high position worldwide such as, inter alia, merchant shipping and financial services.

1.5. Objectives

This Strategy and the Actions set out in chapter 3 below, promote the following key objectives:

- supporting the state's objectives set in the strategic project 'Digital Cyprus' for the development of appropriate conditions for the promotion and support of the Information Society,

- supporting the achievement of the objectives of the Digital Strategy of Cyprus, with particular emphasis on the field of Network and Information Systems Security, and indirect support of its other activities,[3]
- institutionalising cooperation between public bodies and competent authorities (Infrastructure Security, Cybercrime, Cyber Defence and International Cooperation), and enhancing cooperation between competent authorities, critical information infrastructures and businesses (including small and medium-sized enterprises (SMEs) and Start-ups),
- the ability to support national plans for the protection of critical information infrastructures (CIIs) and more broadly the protection of critical infrastructure protection (CIP),
- maintaining and developing an electronically insured business environment in Cyprus, promoting public-private cooperation, and creating and developing ecosystems to promote Cybersecurity at a sectoral level,
- the building of trust by citizens and businesses/organisations in the security of digital Government, including maintaining the confidentiality of information during its transfer, processing and storage.
- informing society on sensitive cybersecurity issues, and establishing a secure electronic environment in the Republic of Cyprus for all its citizens,
- promoting and strengthening training and educational programs for pupils, students, employees, professionals and citizens from all walks of life at all ages to the greatest possible extent,
- promoting and strengthening research and innovation programs in the field of Cybersecurity, promote academic and other,
- reducing or even avoiding the negative impact of cyber threats and effectively responding to emergencies,
- supporting the objectives of the General Data Protection Regulation (GDPR), and in general on privacy issues, as well as balancing regulatory interventions between security and privacy.

1.6. Guiding Principles

The structure and content of this document is based on the following guiding principles:

- the realization of the vision of the strategy for the entire state and for the whole society,
- the overall understanding and analysis of the digital environment, and the adaptation of actions to the specific conditions of the country and the priorities of the state,
- actively involving all stakeholders in implementing the strategy and addressing their needs and responsibilities,
- the development of close cooperation and synergies between the actors involved, and between the competent authorities at all necessary levels, taking into account the responsibilities of the services involved, and the required collaborations at national and international level, the development of a holistic approach to responding to cyber threats, enabling the effective management of cyber risks and promoting the resilience of economic and social activities,
- recognising that a proper strategy must contain multiple layers of security (layered security, defence in depth),
- the use of open procedures at all stages of the implementation of the Strategy, and the use of available policy instruments for the implementation of each of the objectives of the strategy, taking into account the specific circumstances of the country,
- the setting of high targets at the highest level of government and the demonstration of will by the state so that the Strategy and its Actions truly contribute to the definitive change and improvement of the level of electronic security in Cyprus as well as to economic and social prosperity, maximizing the contribution of ICT to sustainable development and social cohesion,
- the responsible assignment of the relevant roles and responsibilities and the allocation of adequate human and financial resources,
- respect for fundamental human rights and values.

---

3 http://www.mcw.gov.cy/mcw/dec/dec.nsf/all/0BACA0B7B7848D2CC22579B500299BFA/$file/Main%20document%20digital%20strategy.pdf?openelement

1.7. Priority Areas

This Strategy is analysed in individual priority areas that have been identified for the optimal protection of critical information infrastructures, the safe use of new technologies and the achievement of a high level of cybersecurity. The priority areas in relation to the needs of the Republic of Cyprus are the following, as shown in Figure 1:

- **building of trust between all those involved** in the implementation of the Strategy, in order to ensure proper and effective cooperation,
- **extension of the legislative framework** by the competent state services covering all aspects of cybersecurity, including cybercrime and the protection of personal data,
- **development of technical and organisational measures and procedures** (in relation to preparation, protection, detection and response to incidents), in order to increase the security of physical spaces, computer and communication facilities, equipment and software, to the extent required,
- **developing the necessary capabilities in organizations and businesses as well as in state agencies on** cybersecurity issues,
- **efficient cooperation of the state with competent bodies of the public and private sector,** both at national and international level,
- **creation or adaptation of the necessary structures and mechanisms** within the competent services and more broadly within the Republic of Cyprus, in order to ensure the requirements and capabilities of immediate response to cyber incidents and crises,
- **Promotion of Research and Innovation** so that the state is able to address, to a satisfactory extent, the rapidly evolving threats from cyberspace, and consequently the developments in the field of cybersecurity to upgrade the security of the critical information sectors of the Republic of Cyprus.

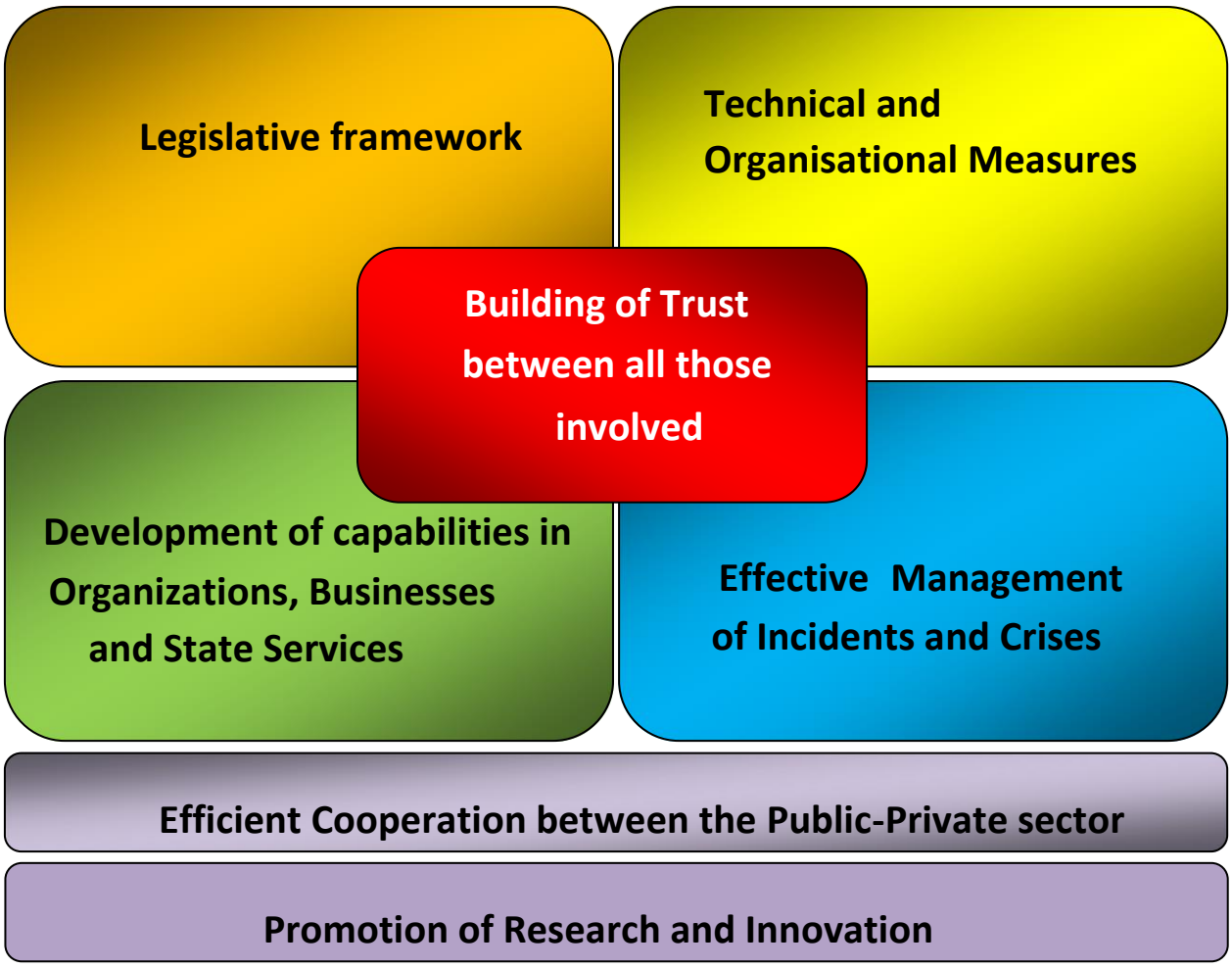


Figure 1: Priority Areas of the Cybersecurity Strategy of the Republic of Cyprus

2. CYBERSECURITY ENVIRONMENT

2.1. European policy

Security issues are an important pillar of the Digital Agenda for Europe. Given the technological changes and the ongoing digital transformation, as well as the increase in cyber challenges and risks, this European policy covers important issues related to the security sector:

- The main objective is for citizens/society, businesses (including small and medium-sized enterprises, SMEs) and public administrations to have secure access to the latest digital security technology, taking into account interoperability, competition, reliability and respect for citizens' fundamental rights, including the right to privacy. This is achieved by improving cyber risk responses, enhancing infrastructure resilience and cooperation between competent authorities and Member States in the area of network and information systems security.

  It also focuses on the fight against cybercrime, notably tackling crimes committed online through electronic communications networks and information systems. Cybercrime can be classified into Internet-related crimes, online fraud, forgery, and illegal content on the Internet. Important EU legislative actions on cybercrime are:
  - The Directive on attacks against information systems (2013),
  - The Directive on combating the sexual exploitation of children on the Internet and child pornography (2011),
  - The Directive on privacy and electronic communications (2002),
  - The Framework Decision on combating fraud and counterfeiting of non-cash means of payment (2001).

- In addition, the improvement of civil-military cooperation is promoted through synergies between civil and military approaches for the protection of critical state infrastructures and in particular in the fields of research and development. It also focuses on avoiding duplication through closer cooperation between governments, the private sector and academia.

- Emphasis is also placed on issues of international cooperation to promote policies and address cyber challenges taking into account freedom of expression, transparency and the implementation of EU laws, rules and core values in cyberspace.

It is now a common understanding at European level that significant improvement is needed in terms of cybersecurity, at collective level in the European Union (EU) as well as for all Member States, especially in terms of institutionalising procedures, creating appropriate structures, training and education, as well as information exchange and operational cooperation.

Since September 2017, the EU has been formally promoting the revision of the European Cybersecurity Framework. The aim of the EU proposals is to define the policy and targeted actions that will make the European Union a protagonist in the field of cybersecurity and place it in a better position to address cyber threats and the risks that accompany them, with a direct impact on Europe's security and prosperity. The EU considers that its proposals will contribute to strengthening competences in technology and skills, as well as to creating a strong single market. It also aims to prevent and respond to cyber-attacks in practice by strengthening mechanisms to detect, identify and hold accountable those responsible.

The EU's approach is based on three main pillars: resilience, deterrence and defence. In order to meet the new European objectives, the European Union Agency for Network and Information Security (ENISA) will play a key role in the new approach, under permanent and upgraded terms of reference. The revised approach promotes operational cooperation and crisis management at European level, a rapid emergency response mechanism and single European Certification of products and services.

The establishment of a European cybersecurity research and training centre is also being promoted, which will allow better cooperation with industry and other stakeholders and foster innovation at European level. Finally, it is planned to develop a fund to deal with cyber emergencies which is a good initiative to help Member States and all those involved to develop their capabilities/capabilities as well as mutual cooperation.

Currently, the European Union's policy on Network and Information Security is implemented through the transposition into national law of the EU Member States and the implementation of the Directive on Network and Information System Security ([4]EU/2016/1148, NIS Directive).
The NIS Directive aims to ensure a uniform minimum level of cybersecurity throughout the European Union. By implementing the Directive, the Member States, ENISA and the Commission should ensure that the following are implemented as a minimum:

- National Strategy for the Security of Networks and Information Systems / Cybersecurity as well as a cooperation framework
- National Computer Security Incident and Incident Response Team – National CSIRT) in all Member States
- Creation of an EU-level NIS Cooperation Group
- Creation of an EU-wide CSIRT Network
- Security requirements and incident notification mechanism
- Identification of "operators of essential services[5] at national level
- Encouraging standardisation.

The NIS Directive applies at least to operators of essential services in critical areas such as:

- Action
- Transport
- Banking operations
- Financial Markets Infrastructure
- Health
- Supply and distribution of drinking water
- Digital infrastructure as well as "digital service providers", such as:
    - Online shopping
    - Online search
    - Cloud computing services.

Member States are free to extend the scope of the Directive in their own country, in relation to the designation of operators of essential services/critical information infrastructures, according to national peculiarities.

2.2. Cybersecurity in the Republic of Cyprus

The Republic of Cyprus has recognized the essential role of security issues in the promotion of new communications services, in the use of new technologies and in general in the development of the information society. To this end, multiple actions and policies have been promoted over time, are being promoted at the present time and are planned for the foreseeable future at national level and in cooperation between all competent authorities and stakeholders in the Republic of Cyprus. For the purposes of completeness and easy reference, previous actions in the field of Network and Information Security and Cybersecurity are set out in Annex II.

In relation to the current situation and specifically since April 2018, the legislation (Law 17/(I)2018) on the Security of Networks and Information Systems was introduced in the Republic of Cyprus, on the basis of which the Digital Security Authority was established under the Commissioner for Communications, and which has been designated as the competent authority for the implementation of the NIS Directive) in the Republic of Cyprus and the coordination of actions for the implementation of the National Cybersecurity Strategy, which includes the operation of the

[4] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[5] The term "operator of essential services" in the Directive NIS It is almost identical to the term 'critical information infrastructure' as found in this document.
[5] The term “operator of essential services in NIS Directive is almost identical to the term “operator of critical information infrastructure” as it appears on this document.

National CSIRT. The initial Law was replaced in August 2020 by the new Security of Networks and Information Systems Law (Law 89(I)/2020). The new legislation gives all the powers to the Commissioner and the Digital Security Authority to implement the NIS Directive, while all the above-mentioned powers of the OCECPR are transferred to the Digital Security Authority (DSA). The specific policies are set out in decisions of the Council of Ministers:

i. on 22/10/16 the Council of Ministers approved the establishment of the National CSIRT (decision no. 81.477) (see article 9 of the NIS Directive),
ii. on 3/5/2017, the Council of Ministers approved the Table, with the information infrastructures in the Republic of Cyprus, which have been designated as "critical", for cybersecurity purposes (decision no. 82.518),
iii. on 20/6/2017 (decision no. 82.816) and 28/6/2017 (decision no. 82.898) it decided:
    - To designate the Commissioner as the national Competent Authority under Article 8 of the NIS Directive, and
    - To create a structure, under the Commissioner, that will function as a national Competent Authority.

With the latest specific harmonising legislation of 2020, the harmonisation with the full framework for Network and Information Security and Cybersecurity has been achieved as well as the definition of the responsibilities and powers of the Authority in accordance with the NIS Directive and the Directive on the Electronic Communications Code in matters of Security.

Since March 2020, the Deputy Ministry of Research, Innovation and Digital Policy has been established in accordance with the Establishment of a Deputy Ministry of Research, Innovation and Digital Policy and the Appointment of a Deputy Minister of Research, Innovation and Digital Policy under the President and Related Matters Law of 2020 (Law 14(I)/2020). The management of policy issues in the field of Digital Security and Cybersecurity have been transferred to the Deputy Ministry. The Deputy Minister defines or revises the general policy framework in relation to digital security. The Authority should act impartially and independently, implementing the relevant general digital Security policy framework.

The new legal and regulatory framework for Network and Information Security and Cybersecurity is complemented by the publication of secondary legislation by the Digital Security Authority which focuses on the better implementation of the Legislation at national level, and the relevant Directives and Regulations of the European Union at national and European level. It is expected that the regulatory framework will be dynamically adapted, in cooperation and consultation with stakeholders, in order to address changing cyber challenges. The competent and/or involved authorities and observers in the Republic of Cyprus are set out in Annex III of this Strategy.

The Republic of Cyprus, in cooperation with stakeholders, and through the work of European bodies, looks forward to actively contributing to the promotion of European policy objectives and international cooperation to address cyber risks and challenges.

2.3. Cyber Threats Today

The use of communication systems and computers[6] have penetrated and now affect almost all the activities of our lives. Technologies are currently used in many critical sectors of our society beyond computer systems and communications and internet services, such as energy production and transmission, water/sanitation system management, financial services, armed forces, security forces, government departments and services, health services, transport, digital infrastructure, etc. Even though the benefits that have accrued from the use of new information and communication technologies (ICT) are enormous and multidimensional, their exploitation is accompanied by a multitude of security issues.

In recent years, multiple cyber threats and risks have emerged. ICT can be used maliciously in illegal activities such as stealing money from bank accounts, accessing confidential, sensitive and personal information, causing damage to important websites (with consequent denial of public access), and even material damage to critical facilities, endangering even human lives. After cyberattacks companies, organizations and government agencies have lost valuable information such as confidential contracts, product designs, credit card information, account numbers, and

[6] Not just classic desktop or laptop computers – we now use a wide range of products that are essentially small computers: smart phones and watches, home appliances, cars, tablets, game consoles, TVs, control systems in homes and hotels, and much more.

other business information. Such incidents can cause serious damage to an organization, since in addition to direct damage, its good name and the trust of its customers are also affected.

The frequency and complexity of cyber-attacks is increasing while many businesses are starting to experience their effects that can affect their business activity. The public, in most cases, is not aware of the results of these attacks, as well as of the type of damage caused by them. Threats are constantly evolving, and many forms of malware appear daily (ransomware, advanced persistent threats (APTs), Distributed Denial of Service (DDoS), and more). In addition to the impact on people and businesses, problems can easily arise in the states themselves. The stability, strength and safe operation of a state is now fully dependent on the smooth operation of its infrastructure, and as can be seen from the above reports, cyberattacks cannot be ignored by anyone.

3. Strategic Response

The strategic response of the Republic of Cyprus to the aforementioned threats, in order to achieve the objectives and vision of this Strategy, is analysed in this chapter. The structure of the Strategy of the Republic of Cyprus consists of overarching themes which have been prepared based on the guiding principles and given the priority areas mentioned in sections 1.6 and 1.7 respectively. For the purposes of this document, which is limited to capturing the political and strategic planning of the state, each Thematic Unit that is briefly analysed in this section, incorporates a series of strategic objectives, and focuses on a number of actions to achieve the purpose, vision and objectives of the Strategy.

Each action will be analysed and costed in the implementation phase of the Strategy and specifically at the stage of planning and preparation of the project plan, where the individual objectives and the expected impact from the implementation of each action will be determined separately, while in the same phase the individual activities and its deliverables will be identified. Also during the same phase, all interested parties and stakeholders involved will be identified that will participate in the implementation phase, a risk assessment will be carried out, while the supervision mechanisms of the specific activities will be recorded, as well as the indicators for measuring its successful implementation. Section 4 gives a more detailed description of the management mechanism of the Strategy and its actions.

The strategic objectives of the Strategy are classified and summarized below. In each Thematic Unit that follows, the general description of each Action is given. It is noted that the Thematic Units are not necessarily independent of each other, while several of the activities within the Actions may fall under or be linked to more than one Thematic Unit and strategic objectives. The strategic objectives can be summarised as follows:

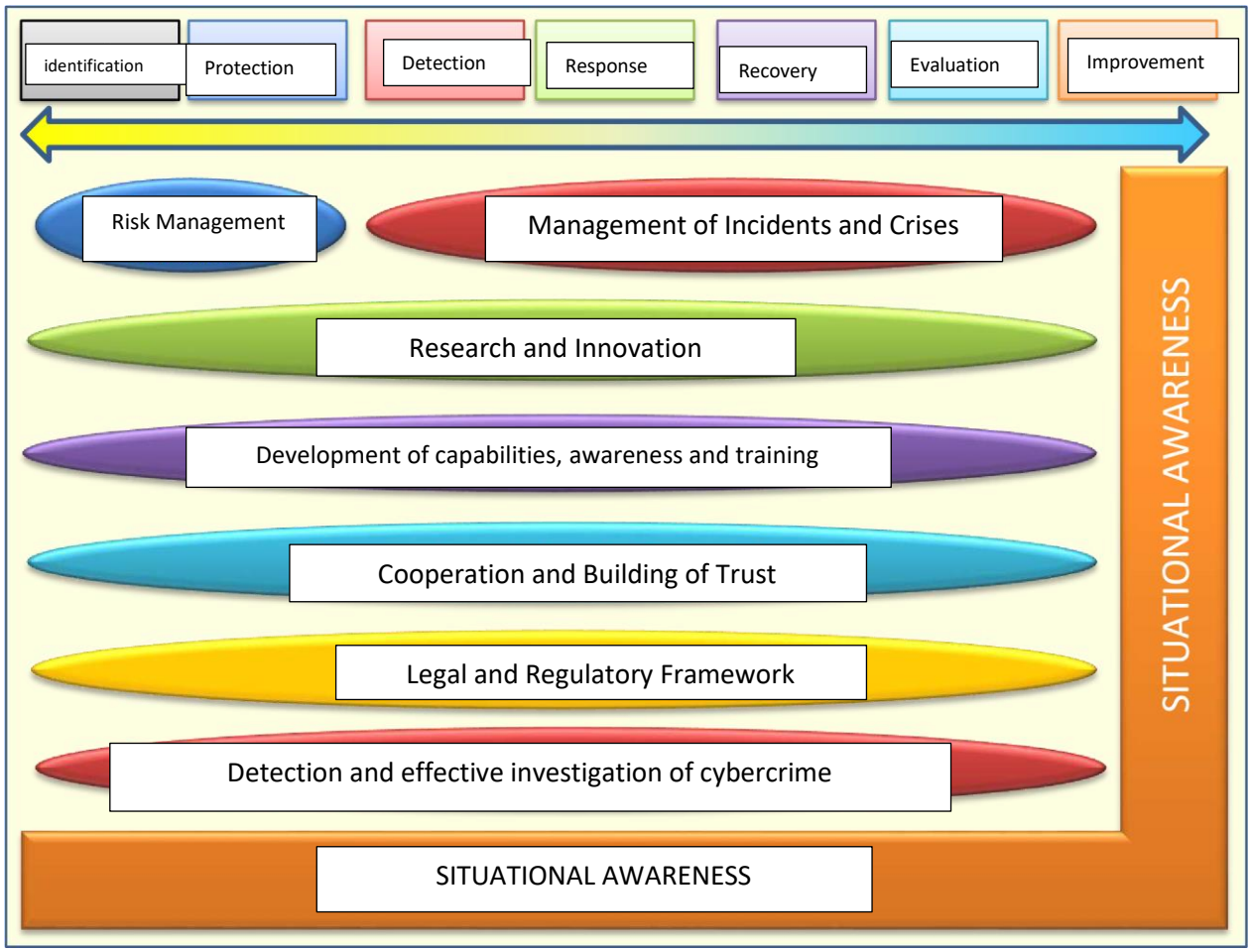
- **Development of Cooperation** and **Trust** - Creation of the appropriate structures for cooperation at all levels and with all the necessary stakeholders, inside and outside Cyprus.
- **Situational Awareness** – Exchange of information, along with analysing it and drawing conclusions about the cybersecurity situation in real time, at technical, operational and strategic level.
- **Risk Management** – Identification of threats, vulnerabilities and risks at all levels, with their appropriate management.
- **Incident and Crisis Management** – Incident management, technical/low-severity incidents (Major incidents, Crisis management).
- **Capability Development** – Continuous development of the necessary capacities and capabilities in the state, organizations, professionals and citizens, in order to support all activities of the Strategy.
- **Education, Training and Awareness** – Special emphasis on the development of security awareness and culture in all strata of society as well as on the specialized education and training of professionals in the field.

- **Research and Innovation** – Innovation to strengthen Cyprus' strengths in key sectors where it is a pioneer, such as financial services and shipping, by supporting research and other funding opportunities from various sources, and creating cybersecurity ecosystems.

- **Legal and Regulatory Framework - Development of a legal, regulatory and** regulatory framework to protect society from threats and cybercrime and to promote a safe environment for the use of new technologies, in accordance with the principles of inclusiveness in an environment of trust.

- **Reduction and effective investigation of cybercrime –** Combating child pornography, illegal access to computer data, racist comments online, financial fraud, extortion via the Internet, as well as other offenses as criminalized by our national legislation.

To better understand the activities identified in the Strategy, Figure 2 shows how strategic objectives can contribute to commonly accepted/implemented actions[7] to address cybersecurity threats and incidents.



[7] Identify – Identify infrastructure assets, threats, vulnerabilities, risks, and other important elements to understand the cybersecurity environment.
Protection (Protect) – Protection of infrastructure, services and information based on the risks identified (risk management).
Detect – Detect incidents when they occur, including attempts at attack.
Respond – Management of incidents, whether they are simple technical incidents, or some form of operational or strategic / political crisis.
Recover – Recovery after a successful attack, and return to normal operating levels.
Evaluate – Evaluation of the results of the Strategy's Actions, to understand their impact on cybersecurity levels in Cyprus.
Improve – Improve actions and their results, as well as recommendations for improving cybersecurity levels in Cyprus.

Figure 2: Thematic Strategy Units in relation to the cybersecurity response cycle

Furthermore, Figure 3 shows the relationship of the Thematic Units with the Priority Areas of the Cybersecurity Strategy of the Republic of Cyprus, referred to in section 1.7 of this document, in order to better understand the structure and the main pillars on which this strategy is based.

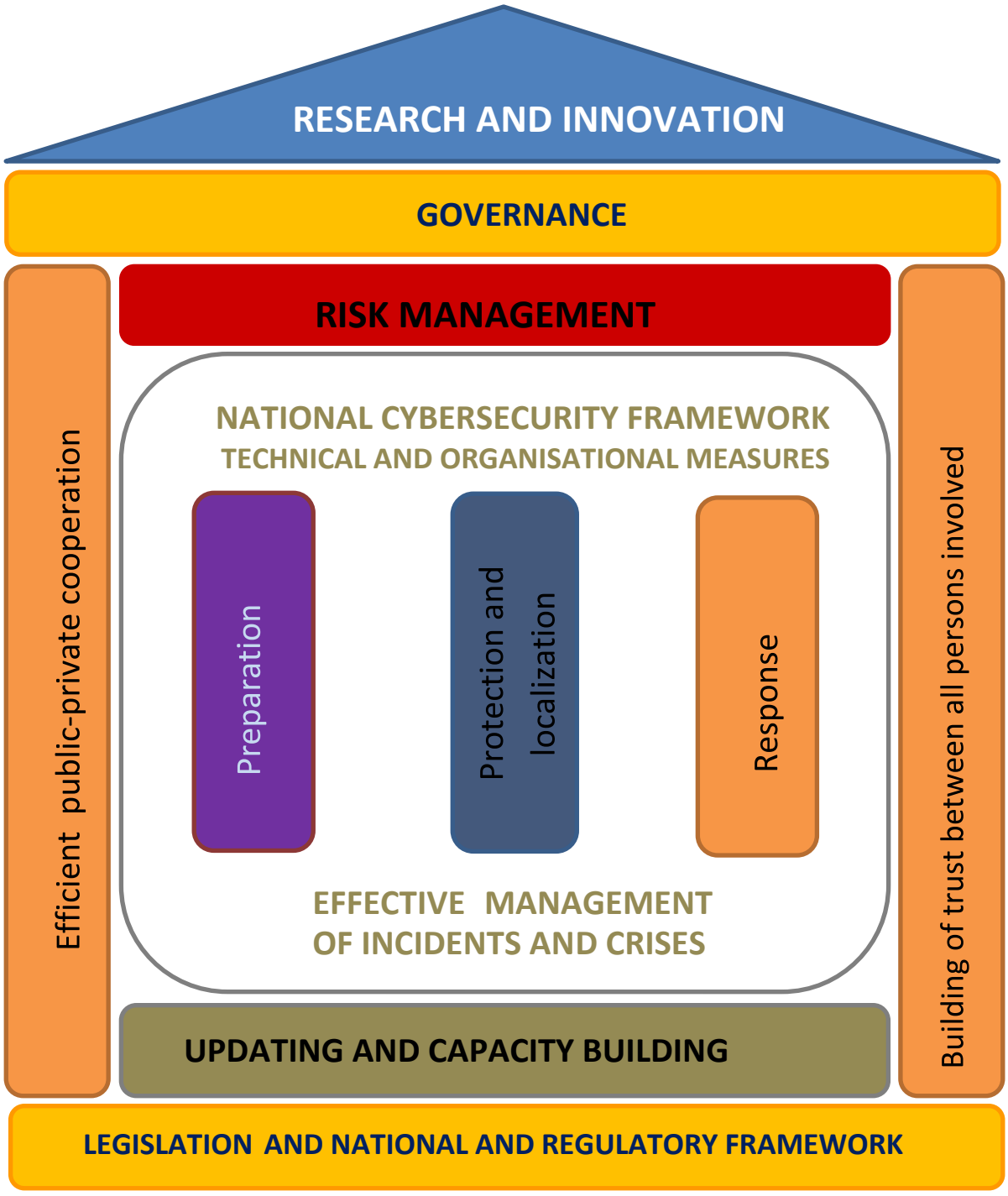


Figure 3: Relationship of Thematic Units with the Priority Areas of the Cybersecurity Strategy of the Republic of Cyprus

3.1. Thematic Unit 1 – Structures and Governance

Strategic objectives: General Action Covers all objectives

Cybersecurity is a large and complex chapter in terms of security governance in a state, and requires the involvement of a large number of public sector bodies. Each competent body has its own areas of responsibility and it is important to maintain clear roles. Due to this multifaceted involvement in the management of the individual aspects of cybersecurity, it is imperative that it is understood and accepted by all that maintaining security in cyberspace can **only** be achieved with the efficient cooperation of the stakeholders in the context of a unified and coordinated response to the various threats already mentioned.

Therefore, the coordination of the competent bodies of the state becomes necessary. In the Republic of Cyprus, several steps have been taken in recent years (see section 2.2) towards development of capabilities in cybersecurity, and more institutionalised coordination and delegation of responsibilities in this area is necessary.

This activity is efficient when it is done on the basis of a mechanism that coordinates the efforts of the Republic of Cyprus, holistically, for its excellent response to the threats that appear today as well as the emerging cyber threats.

Based on the existing legal framework, the **Deputy Minister of Research, Innovation and Digital Policy to the President, defines or revises the general policy framework** in relation to Digital Security in Cyprus.

Also on the basis of the same legal framework, the **Digital Security Authority (DSA) has been created**, as a result of the activities for the creation of a national independent cybersecurity structure in Cyprus, including the obligations of the Republic of Cyprus under the NIS Directive (see Thematic Unit 3), headed by the Commissioner for Communications[9] (see Thematic Unit 2.2), and which is responsible for:

- the coordination of the implementation of this Strategy, under the political supervision of the Deputy Minister and on the basis of the strategic and political decisions of the National Cybersecurity Council, through structured program management (Strategy Programme Management – see Thematic Unit 4), including the coordination of some Actions of the Strategy,
- the full implementation of the NIS Directive, through the exercise of the relevant powers of the Authority described in the applicable Legislation (see Thematic Unit 3),
- the operation of the National CSIRT (Computer Security Incident Response Team) (see Section 6),
- cooperation and support of the Deputy Ministry in defining and reviewing digital security policy and cooperation with the competent authorities on individual cybersecurity issues (cybercrime, cyber defence, relevant external relations) (see Thematic Unit 1 and module 2),
- cooperation in the framework of other relevant activities at national level, e.g. Basic National Plan (BNA) "ZENON", SENDAI Framework,[10] National Security Strategy, risk assessments at national level, etc.).

In exercising its powers, the Authority shall:

- act impartially and independently by applying the relevant general policy framework referred to in the previous paragraph;
- have the **appropriate legal authority and defined competence** to be able to carry out its work,
- have the **necessary know-how** to properly meet the obligations of the role,
- have the **necessary links** and maintain **good working relations** with the competent state bodies, the operators of critical information infrastructures of Cyprus, the private sector stakeholders, and the international working groups and forums on the issue.

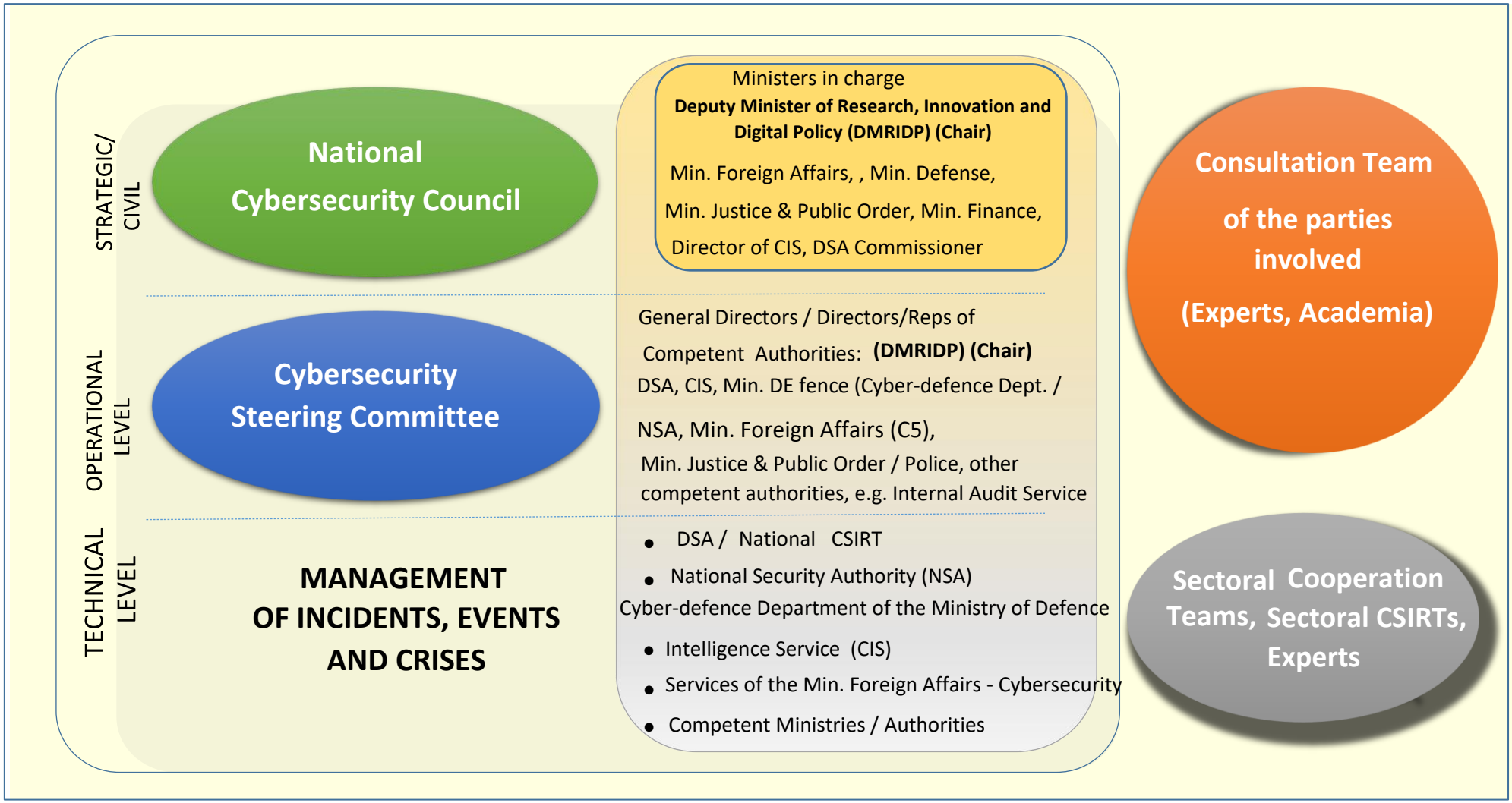
[9] The term Commissioner for Communications is a renaming of the term Commissioner of Electronic Communications and Postal Regulation on the basis of a relevant decision of the Council of Ministers and an amendment of the Law on the Regulation of Electronic Communications and Postal 112(I)2004.

[10] http://www.unisdr.org/we/coordinate/sendai-framework

- have the **necessary resources** and mechanisms such as political will, funding, time, and staff.

This Action will examine the creation of the competent bodies and groups, aiming at the better implementation of the Strategy, as well as the more effective response of the Republic of Cyprus against cyber threats (see Figure 3):

- **National Cybersecurity Council**, with high-level representation from the main competent authorities involved, at the level of Minister / Governor / Commissioner as follows: network and information security (Deputy Ministry of Research, Innovation and Digital Policy and Digital Security Authority), cybercrime (Ministry of Justice and Public Order, Cyprus Police), cyber defence (Ministry of Defence, National Guard General Staff, National Security Authority), international cooperation (Ministry of Foreign Affairs), cybersecurity expenditure (Ministry of Finance) and Intelligence Services (Cyprus Intelligence Service). The chairmanship of the body will be assumed by the Deputy Minister of Research, Innovation and Digital Policy to the President, who will be supported by the Digital Security Authority to monitor the implementation of the Strategy, as the competent Authority for coordinating the implementation of the Strategy. The body will monitor the progress of the implementation of the Cybersecurity Strategy at regular intervals (e.g. every 6 months or 1 year), will be informed about the current cybersecurity situation in the Republic of Cyprus, and, where necessary, will give guidelines for the improvement of cybersecurity in general. Furthermore, this body will be convened in cases of major cybersecurity crisis, which affects the Republic of Cyprus at national level, in accordance with the current crisis management plans of the Republic for Cybersecurity.



Grapha 1 : Government security structures in the Republic of Cyprus

- **Cybersecurity Steering Committee**, with representation by the same stakeholders as in the National Cybersecurity Council, at the level of General Directors and/or Directors of services and/or sector managers and/or their authorized representatives, as well as corresponding representatives of other authorities whose participation is deemed useful, by decision of the President and the Cybersecurity Steering Committee. The Presidency of the Committee will be held by the Director General of the Deputy Ministry of Research, Innovation and Digital Policy, who will be supported by the Digital Security Authority in relation to the Committee's activities in order to monitor the implementation of the Strategy. In this body, the interdependencies will be recognized and the cooperation between the competent authorities of the Republic will be ensured so that the knowledge of the experts / technocrats in each authority will be used to the maximum extent. This Committee will also examine the interdependencies and interactions between the individual strategies of the competent authorities and the actions proposed and/or promoted, even though each one has its own specific and distinct objectives, for the purpose of their successful implementation as well as for possible synergies and the avoidance of overlaps. The matter of strategic response to cybersecurity threats should be addressed holistically and it is necessary to understand that several of these Actions need to be implemented in a combined manner, with the aim of maximizing the success of such a response. Furthermore, this body will be convened in cases of a cybersecurity crisis which affects the Republic of Cyprus to a large extent (see section 3.7), in accordance with the Republic's applicable crisis management plans for Cybersecurity.

- **Stakeholder Advisory Group**, with the representation of stakeholders (such as e-commerce and e-government), academic institutions, operators of essential services, operators of critical information infrastructure, electronic communications providers, digital service providers, non-governmental organizations, relevant companies and other private sector organizations. In general, there should be a feedback mechanism for all relevant stakeholders regarding the implementation of this Strategy. At regular intervals, the results of the Actions taken within the framework of the Strategy will be presented, as well as the planning and focus on next activities, for the purposes of providing information and guidance to competent authorities, where required.

- **Sectoral Cooperation Groups**, **and possible creation of sectoral structures (e.g. sectoral CSIRTs)** for cooperation, coordination and exchange of information as well as for the most efficient and specialized response to incidents, within the critical sectors which are defined by the Council of Ministers, in order to maintain the essential functions of the state and society.

- **Working Groups** for the successful implementation of the Strategy's Actions. These groups will be set up according to the needs of each Action, whenever necessary.

The cooperation between the main competent authorities on network and information security, digital security, cybersecurity, cybercrime, cyber defence and related external relations will take into account the fact that several of the Actions described in this Strategy are of a horizontal nature. At the same time, in the planning of each Action, other activities that the competent authorities will implement, in their areas of competence, will be taken into account.

Actions:

Action 1 - Creation of appropriate structures and teams for the successful implementation of the Strategy, and to effectively deal with emerging threats in cyberspace, as well as emerging threats that will appear in the future. Where deemed necessary, the need to create new or to strengthen existing structures (e.g. sectorial CSIRTs) and partnerships will be considered, in order to maintain high levels of cyber security in the Republic of Cyprus. For all work that will be carried out within the framework of the Strategy, interdependencies will be taken into account wherever they occur.

3.2. Thematic Unit 2 – Institutionalisation of cooperation between competent public bodies

Strategic objectives: Cooperation and Trust Building, Understanding of the Situation, Risk Management, Incident and Crisis Management

The main objective of the Strategy is the creation of a mechanism for the identification and integration of government bodies which are affected or in charge of its implementation. The achievement of intergovernmental commitment, efficient coordination and continuous cooperation should be the key functions of these government institutions, and which are required in order to ensure that governance mechanisms which are mentioned in Thematic Unit 1 and the resources available to the Republic of Cyprus, deliver the desired results which are aimed by the Strategy.

Effective communication and coordination ensure that all ministries, competent authorities and government services are aware of the mission, responsibilities and duties of the competent authorities and government services dealing with relevant cybersecurity issues. The commitment and consistent implementation of the state's policy by all competent authorities and state services on an ongoing basis, are necessary elements in order to ensure the fulfilment of the vision and objectives of the strategy.

In the context of the institutionalized cooperation of the competent public bodies, special emphasis will be given, by all stakeholders to the implementation of the provisions of the Cybersecurity Package[11] which was issued by the European Commission in September 2017. The Digital Security Authority will cooperate with the competent authorities to the maximum extent possible, within the framework of its functions, in order to support the objectives of effectively combating cybercrime, preventing cyber-attacks, developing cyber defence capabilities, and strengthening international cooperation on cybersecurity. In particular, competent authorities should take measures, inter alia, concerning the following:

- Identification of perpetrators of malicious actions;
- Strengthening the legislative and regulatory framework;
- Public-private cooperation in the fight against cybercrime;
- Strengthening cyber-attack response mechanisms at political level;
- Enhancing deterrence capabilities through defensive tools;
- Inclusion of cybersecurity in the context of building international relations;
- Developing capacities, capabilities and partnerships in the fields of cybercrime, cyber defence and international cooperation;
- Ensuring coherence between the country's national and foreign policy, so that one ministry and/or one state service does not undermine the credibility of the other, representing different positions in the same policy area;
- Assisting in efforts to consolidate stability in cyberspace;
- Identifying and countering hybrid threats.

[11] Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, http://eur-lex.europa.eu/legal-content/EN/.TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

Action:

Action 2 – Creation of a mechanism for the coordination of Ministries, competent authorities and state services involved, on the basis of the structures which are mentioned in Thematic Unit 1, with main aim, inter alia, the carrying out of periodic meetings in which all interested parties will participate in order to inform them about action plans concerning state services, cooperation and coordination of actions.
An example of a cooperation mechanism would be the creation of a dedicated working group to address a specific issue.

3.3. Thematic Unit 3 – Legal, Regulatory and Political Framework

Strategic objectives: General Action, Covers all objectives

The matters of cybersecurity and cybercrime are adequately covered by legislation applicable in the Republic of Cyprus. Nevertheless, there is still a need to constantly update and modernize **all** relevant legislation, as well as the need to promote new primary and secondary legislation for the purpose of harmonization with any newer European legislation, as well as to cover special provisions under this Strategy. Special emphasis will be placed on the obligations stemming from the NIS Directive, the upcoming revision of the electronic communications legislation on network and information security, the new Regulation on the European Union Agency for Network and Information Security (ENISA), the European legislation that is expected to result from the implementation of the New European Cybersecurity Package) including cybercrime issues[12], the General Data Protection Regulation (GDPR), and more generally as a result of issues regarding privacy and safeguarding fundamental rights (in case of criminal investigations and prosecutions), in accordance with the principle of fundamental human rights, and many more.

In particular, the NIS Directive, (EU) 2016/1148 on the security of network and information systems across the European Union (see section 2.1) represents the first horizontal EU piece of legislation to address cybersecurity challenges and constitutes a real breakthrough for cybersecurity resilience and cooperation in Europe. The Republic of Cyprus is fully committed to achieving the objective of a high common level of security of network and information systems in the European Union, which is considered absolutely necessary for both the political and operational levels represented by the infrastructure established in Cyprus (see section 3.1). This Thematic Unit gives emphasis to the effective implementation and enforcement of the relevant Cyprus Law.[13]

The strategy encourages the creation of a process to monitor the implementation and review of legislation and legal governance mechanisms, to identify gaps and overlapping competences, and to identify and prioritise areas that need modernisation.

Cybersecurity matters require European and international cooperation with other Member States of the European Union and possibly with third countries. Therefore, legal issues may arise in the processing and handling of electronic threats that may originate from sources outside the boundaries of the Republic of Cyprus. Therefore, it is considered necessary to create the appropriate legal background for effective cooperation with institutions inside and outside Cyprus, in order to solve problems when they arise. In this Thematic Unit, legal tools will also be examined with which the state can promote specific measures, with the aim of improving the levels of cybersecurity

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[13] Law 17(I)2018 and any Law amending or replacing it.

in all sectors, whether they are considered critical or not. Examples of this is the provision of various incentives to small and medium-sized enterprises to develop their cybersecurity capabilities and levels, through certification programme of organisations or by providing access to government and funded projects only to companies that comply with minimum levels of cybersecurity. Different ways of providing incentives will also be considered, led by the Stakeholder Advisory Group (see section 3.1).

The Thematic Unit includes the establishment of national compliance mechanisms (for both enforcement and incentives). These mechanisms should be established to prevent, combat and mitigate actions against the confidentiality, integrity and availability of ICT systems and infrastructures, and by threatening computer data, in accordance with the national and European legal framework.

Finally, under this Thematic Unit, the strategy encourages the development of cyber law enforcement capacities, including the training and education of various cybercrime actors involved (e.g. judges, prosecutors, lawyers, police officers, forensic scientists and other researchers). Law enforcement authorities need to receive specialised training in the interpretation and application of national and European legislation in the field of cybercrime, in order to effectively detect, prevent, investigate and prosecute cybercrime and to cooperate effectively with industry and international law enforcement actors (e.g. INTERPOL, Europol) in order to tackle cybercrime and strengthen cybersecurity (see Thematic Unit 14 and Thematic Unit 15). This should take into account Thematic Unit 10 on education, training and development of capabilities and Thematic Unit 9 on awareness and information.

Actions:

Action 3 - Full implementation of all provisions and regulatory framework of the NIS Directive, at all levels, with emphasis on critical information infrastructures and operators of essential services.

Action 4 - Strengthening the existing legal and regulatory framework for the full activation and support of the provisions of the Cybersecurity Strategy, and the creation of new legislation where necessary. All relevant legislation of the competent authorities should be examined if there is a need for adaptation. The legal framework for cooperation and information sharing with third countries and private sector organizations should be considered, as well as the promotion of a possible policy framework to incentivize businesses to upgrade and strengthen cybersecurity levels in their infrastructures. A process for monitoring the implementation and review of the legislation as well as compliance control mechanisms should be revised or established.

3.4. Thematic Unit 4 – National Cybersecurity Framework

Strategic objectives: Risk Management, Development of Capabilities

This Thematic Unit provides for the development of a comprehensive National Cybersecurity Framework, which is one of the main activities of the Cybersecurity Strategy of the Republic of Cyprus. It concerns the prevention of cyber incidents with adverse effects at national level. The National Cybersecurity Framework aims to define how the various services and departments of the Public Service, as well as the operators of critical information infrastructures, will manage cybersecurity-related risks. The aim is to extend the existing framework that can be

used by each operator, regardless of the degree of sensitivity and value of the information it handles. Indicatively, the full National Cybersecurity Framework will include, inter alia, activities such as:

- Defining the value and sensitivity of information and infrastructure
- Risk assessment and management
- Vulnerability analysis and management
- Definition of possible security measures (security controls)
- Methodology for the selection of security measures
- Application of security measures
- Penetration testing
- Review and compliance audits.

The National Cybersecurity Framework may contain a large number of security measures, but these will not necessarily be applicable in all cases. Therefore, the Framework will include a methodology for selecting security measures, in order to select and apply as many security measures necessary for each case, always based on the results of a proper and structured risk assessment. Where possible, the use of relevant standards which where, developed with good practices in mind, for effective protection against cyber threats, will be promoted.

The specific objectives of this Action can be summarised as follows:

1. The effective and continuous strengthening of the shielding of the networks and information of the Public Service, the Wider Public Sector and the Critical Information Infrastructures from relevant cyber threats.
2. Development of a single methodology for use in all sectors, allowing comparable levels of security, based on the needs of each service / department / organization / business.
3. A framework that allows measurable results of audits and evaluation for cybersecurity levels in the Republic of Cyprus.

It is noted that the specific objectives that will be set in terms of the levels of protection of the systems mentioned in this Thematic Unit, will be determined by the analysis of the risk assessment in each sector and taking into account the cost of implementing the specific measures in relation to the benefit in dealing with the relevant cyber threats.

Action:

Action 5 - Development of a National Cybersecurity Framework that will promote the protection of critical information infrastructures in the Republic of Cyprus, as well as of all government services of the state.

3.5. Thematic Unit 5 – Risk Assessment and Management – Criticality Assessment

Strategic objectives: **Risk Management**

The framework of measures for the protection of critical information infrastructures, as highlighted and explained in this document and in particular in Thematic Unit 4 above, is necessary to minimize the negative effects and catastrophic consequences of possible malicious actions or natural disasters on infrastructure, at national level within the Republic of Cyprus. Furthermore, as follows from the obligations of Cyprus in relation to the applicable European law, the framework is necessary to address possible impacts on the infrastructures of other countries and/or organizations, due to the great interaction and interconnectedness of the international communication networks and the connection of many critical infrastructures of the Republic of Cyprus with European networks (in the European Union and with other Member States) that it entails.

The approach which is appropriate for the proper design of a security programme should include a structured methodology for understanding risks as foreseen by the NIS Directive. The implementation of risk assessment at national level presupposes that the risks that may affect the Republic of Cyprus at state level must be adequately recognized and understood. A risk assessment should be carried out at regular intervals (e.g. every 2 years) at national level on cybersecurity issues. This activity has already started in Cyprus, and was implemented at national level for the first time in the period of 2015-2016, and will continue during the implementation of this Strategy.

At European level, in recent years, high priority has been given to risk analysis issues at various levels and in almost all sectors. Therefore, the Republic of Cyprus carries out similar analyses in various areas, such as a recent Civil Defence project (in progress), which analyses the risk in a number of areas related to the Essential National Plan "ZENON" (floods, earthquakes, interruption of communication networks, etc.). the regular performance of a cybersecurity risk assessment is consistent with these activities and will provide more comprehensive information to risk decision makers.

3.5.1. Risk Assessment and Criticality Assessment at National Level

Risk assessment at national level aims to develop a national risk register, which is stored and transmitted securely, in order to allow for state oversight of risks and the approaches taken to manage them. The DSA should develop a method of prioritising risks based on an assessment of the likelihood of risks materialising as well as their impact. The risks identified based on the above activities should be systematically monitored, while they will be used as guidance for the implementation of the other Actions of the Strategy.

As part of the process of managing national cybersecurity risks, the question of exactly which infrastructures should be considered 'critical' must be answered. It is necessary to identify and evaluate truly critical infrastructures in the Republic of Cyprus and target them for the best possible protection. These critical infrastructures are identified and evaluated based on the methodology developed in a relevant action of the first National Cybersecurity Strategy, as amended and improved, and this methodology forms an integral part of risk management at national level. To optimise this assessment, relevant risk assessments should be carried out by each actor handling critical infrastructure (see Thematic Unit 3.4 - Cybersecurity Framework).

3.5.2. Risk assessment and risk management at critical level information infrastructures and essential services

The DSA, as the competent authority should define a coherent approach to risk assessment also at the level of critical information infrastructures and essential services, to be followed by all government entities and operators of critical information infrastructures and essential services, identified at national level. The approach should also lead to the identification of key assets and services of critical information infrastructures and essential services, which are critical for the proper functioning of society and the economy, as well as the threats and risks associated with them. In addition, the responsibilities of key actors in each sector in assessing, accepting and addressing national cyber risks should be identified.

The DSA should also define a common methodology for managing cybersecurity risks. This will ensure efficiency and coherence across organisations and facilitate the exchange of risk information between interdependent systems. The methodology may take into account international standards, as it can reduce costs and bring about better interaction with the private sector. The methodology should provide guidance on the assignment of roles and responsibilities for different aspects of risk management, such as threat assessment, asset valuation, implementation and maintenance of mitigation measures and acceptance of residual risk. The methodology should include a certification programme that contributes to the assessment and ultimately to the improvement of compliance. Most importantly, for contracting and developing infrastructure or services, the risk management methodology should also provide guidance on minimising risk through a secure architecture and design, recognising that security is best achieved when it is an integral part of the design process of a product, process or service (security by design).

Actions:

Action 6 - Assessment and management of cyber security risks in the Republic of Cyprus through a structured methodology to identify critical information infrastructures and the risks that may affect them, with an analysis of possible impacts and mitigation options (risk treatment options), as well as continuous improvement.

6.1 The risk assessment will be carried out at regular intervals (every 2 years) to update the results and guide all the Actions of the Strategy, in accordance with the provisions of the NIS Directive and the existing national legislation.

6.2 The criticality assessment will be carried out every two years and/or earlier if the need arises in accordance with the provisions of the NIS Directive and applicable national legislation.

Action 7 - Development of a coherent methodology for risk assessment and management at the level of critical information infrastructures and essential services.

3.6. Thematic Unit 6 – Incident Response and Crisis Management

Strategic objectives: Incident and Crisis Management

Even though the actions mentioned in Thematic Unit 4 (Development of a National Cybersecurity Framework) and Thematic Unit 5 (Risk Assessment and Management – Criticality Management), aim to minimize risks and prevent cybersecurity incidents, the risks, threats and incidents cannot be eliminated. Therefore, and due to the ever-present likelihood of incidents which have adverse effects, it is necessary to ensure incident management capabilities, by developing capabilities for this purpose at national level.

3.6.1. Operation of Cybersecurity Incident Response Teams (CSIRT)

Recently, the National CSIRT [14] (Computer Security Incident Response Team) of Cyprus (CSIRT-CY) has been established, which supports critical information infrastructures in dealing with major cyber incidents and attacks. The main function of a CSIRT is to prevent serious incidents related to network and information security as well as to respond promptly to such an incident if it occurs. It is emphasized that for the proper functioning of a CSIRT, the following are required: a) the necessary infrastructure and b) staffing, training and education of staff. A basic condition for the proper functioning of these services is the practical support by the state. Specialized CSIRT teams should provide a set of both preventive and reactive functions, as well as preventive and educational services. These teams can increase a country's ability to respond quickly and recover from cyberattacks, as well as improve the resilience of the Republic of Cyprus against cyber threats, reducing the potential overall economic and operational impacts critical information infrastructures.

The establishment of the National CSIRT does not mean that other CSIRTs will not operate in Cyprus (e.g. governmental, academic, possible sectoral, etc.), but their operation will be complementary and supervised by the Digital Security Authority. Within this Thematic Area, provision is made for the coverage of the services provided by CSIRTs which will be assessed at regular intervals, and in cases where necessary, the need will be documented and the creation of additional CSIRTs, such as sectoral CSIRTs, will be properly supported, and/or the national CSIRTs will be appropriately strengthened. The needs will be identified in relation to the understanding and situational awareness regarding cyber threats and related incidents in Cyprus, as well as to the strategic plans of the state to promote important sectors of the economy (e.g. merchant shipping, financial services, etc.). The benefits of setting up sectoral CSIRTs in such important sectors of the economy will be examined, and where beneficial their creation will be promoted in integrated planning.

Within the framework of European cooperation in the field of information security, as described in the NIS Directive, the cooperation of CSIRTs operating in each Member State is also included. With the aim of integrating the Cypriot CSIRTs into these cooperation mechanisms, their full operation should be ensured in order to ensure their necessary certification to enable their participation in the European working groups.

A clear framework and procedures should be put in place with details on the manner and the procedures for notifying incidents to the relevant bodies (CSIRTs) in order to be able to properly prioritise the response. This framework should be agreed upon and respected by all stakeholders and include elements in terms of architecture, interfaces and standards for structured information exchange to optimise response to major incidents (see Thematic Unit 3.6 - Incident Response and Crisis Management).

3.6.2. Crisis management

As explained above, no technological system or package of measures and actions, no matter how comprehensive, **can fully protect** cyberspace, and especially the critical information infrastructures of any country. In light of this fact, it is necessary to revise and update the relevant Contingency Plan for Critical Information Infrastructures. The aim of this plan is to guide and develop detailed procedures and measures to be taken when a large-scale crisis significantly affects the operation of critical information infrastructures in the Republic of Cyprus. The plan developed under this Strategy should form part of the general national emergency plan of the Republic of Cyprus. The plans must be aligned with the broader National policy.

The national cybersecurity contingency plan should review the findings from national risk assessments (see Thematic Unit 3.5 - Risk Assessment and Management - Criticality Assessment) and possible cross-sectoral dependencies that could affect the continuity of operations of critical infrastructure, as well as any disaster response mechanism. In addition, it should provide an overview of national incident response mechanisms, as well as identify and classify cyber incidents, based on their impact on critical assets and services. In particular, the creation and development of the Emergency Plan includes the following actions:

[14] http://www.csirt.cy

- development of categories and prioritisation of critical infrastructures, based on their contribution to the maintenance of vital communication and information services and based on the relevant results of regular risk assessment (see Thematic Unit 5 - Risk Assessment and Management - Criticality Assessment),
- development of "early warning" systems and procedures for infrastructure monitoring, with the help of the National CSIRTs,
- establishment (or improvement of already existing) emergency communication networks which are independent of the main networks and, if possible, using another physical means of communication (e.g. wired, mobile and satellite networks);
- development of **comprehensive** communication and crisis management procedures between managers of critical information and communication infrastructures to achieve efficient cooperation between them,
- carrying out regular national exercises with realistic crisis scenarios for testing and improving the above procedures,
- identification of available resources at the level of equipment and infrastructure, where useful or necessary, between the services involved, and the creation of synergies for duplication of resources and mutual support of services in the event of an emergency.

It is noted that the above provisions, where necessary, will be used in the context of Cyprus' contribution to the development of the Rapid Emergency Response Blueprint [15] for cooperation between EU countries and for cooperation with European structures.

Actions:

Action 8 - Consolidation of the National (and other where appropriate - sectoral) CSIRTs in Cyprus, with the development of appropriate information exchange procedures and interfaces, in order to achieve effective incident response and management in the Republic of Cyprus

Action 9 - Development of an updated contingency plan to address cybersecurity crises and its use in all relevant exercises (link to action 11).

[15] http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=3&year=2017&number=6100&version=ALL

3.7. Thematic Unit 7 – Development of capabilities – Organisation and Participation in Exercises

Strategic objectives: **Development of capabilities, Collaboration, Education, Training and Awareness**

3.7.1. Development of capabilities

As part of the activities for the full implementation of the NIS Directive (see Thematic Unit 3 - Legal and Regulatory Framework), operators of critical information infrastructures will have to comply with specific cybersecurity obligations, and will be subject to relevant compliance checks. It is to be expected that not all operators of critical information infrastructures will be on the same level in terms of their capabilities to effectively protect against cyber threats, at least in the early stages of implementation of the Directive.

Therefore, there should be a possibility to support the efforts of such agencies and the ways in which they can be assisted to further develop their capabilities should be studied. As a multifaceted issue, maintaining high levels of cybersecurity requires expertise and multidimensional training, and so it is important to develop capabilities in these areas. At the same time, other organisations will be able to benefit from the relevant efforts to support the parties involved, and the best ways in which the state can support these actions should be studied.

As stated in section 2.3 (Competent Authorities) of the Strategy, there are many stakeholders that need to work together to effectively address cyber threats. An important area of cooperation is also "capability development" It is emphasized that the term "capability development", does not refer only to technical and organizational measures, but also extends to structures, management systems and necessary resources (Thematic Unit 1), such as appropriate human resources and financial capabilities, cooperation issues (Thematic Units 2, 12, 14), appropriate operational planning (Thematic Units 4, 6), the knowledge background (Thematic Unit 10) and the corresponding legal framework (Thematic Unit 3) etc. The DSA should promote measures for the continuous education and training of staff of critical information infrastructures and essential services (Thematic Unit 10), either through initiatives of the Authority or of the organizations themselves. In any event, the DSA should ensure a minimum level of knowledge and capabilities to address cyber challenges.

In addition to the above, the essential rule for "capability development" is the continuous evaluation, simulation of real situations and the control of the correct implementation of business plans, structures, knowledge, the legislative framework and in general all the elements required for the efficient response to threats, risks and incidents in cyberspace. The most efficient way of assessing and controlling the readiness of the teams involved in the management of Cybersecurity issues is to plan and carry out exercises both at national, European and international level.

3.7.2. Organization and participation in Exercises

The strategy encourages the organisation and coordination of national, European and international cybersecurity exercises and response to cybersecurity incidents. These exercises can take different forms (e.g. simulations or real-time exercises) and aim to engage the technical community and decision-makers.

Cyber exercises and other crisis simulation mechanisms can help countries develop institutional capacity to respond effectively to incidents, test crisis management processes and communication mechanisms, verify the operational capability of CSIRTs to respond to pressure, and identify sector interdependencies.

Similarly, European and international cyber exercises can help strengthen cyber response capacity among states, understand cross-border dependencies, build trust between countries and improve the overall international level of resilience and preparedness.

The carrying out of such exercises has also proven to be a very important tool to ensure the preparedness of relevant actors to face a potential crisis, e.g. a loss of a significant part of a large communications network. The exercises carried out in the Member States as well as at pan-European level, have shown that despite the existence of

appropriate mechanisms to deal with such a crisis, the element that is usually missing, in order for the response to a crisis to be effective, are the **details for coordinating cooperation** between the competent bodies (e.g. who will contact whom in case of a crisis, how exactly the rapid cooperation between institutions is achieved, etc.).

The Republic of Cyprus has a lot to gain from organizing and actively participating in such exercises. Of course the benefit is maximised by carrying out similar national exercises with realistic scenarios. The carrying out of such exercises will contribute to maximizing the degree of readiness of the Republic of Cyprus to cope with significant cybersecurity incidents that may affect a large part of the population.

Actions:

Action 10 - Development and promotion of measures, programs and activities to develop real cybersecurity capabilities in the organizations that manage critical information infrastructures, as well as in other organizations and companies, where necessary. These capabilities should cover the full range of cyber security activities - Identify, Detect, Protect, Respond, Recover in the context of continuous improvement.

Action 11- Planning and organizing regular national cyber security exercises, based on realistic scenarios, as well as active participation in Pan-European and other international exercises (link to Action 9).

3.8. Thematic Unit 8 – Exchange of Information – Situational Awareness

Strategic objectives: Cooperation, Situational Awareness, Education, Training and Awareness

3.8.1. Exchange of information

The ever-increasing use of new technologies and the dependence of key functions of a state's economy and society on their exploitation, combined with the consequent increase in threats, risks and complexity of security incidents, increase the importance and severity of potential impacts from cyberattacks, in particular on critical systems. Each organization alone finds it difficult to monitor and analyse the vast amount of information it needs to take into account to address the challenges, threats, risks and vulnerabilities identified, as well as the impact on incidents. International experience constantly highlights the importance of cooperation and exchange of experience and information at all levels. The exchange of information becomes a valuable and irreplaceable tool provided that it is done in a correct and structured way, within the framework of cooperation and mutual trust:

- **Between organizations in the same sector (sector, e.g. energy, transport, etc.).** Many targeted cyber-attacks which are observed usually target organizations in the same sector, e.g. banks. When attacks are observed within Cyprus in one area, it is of direct interest to the other organizations in the same sector for more effective protection.
- **Between organizations across various sectors and DSA/National CSIRT**. Gathering information on threats and attacks centrally, will assist all organizations involved in dealing with such threats, as well as for effective cyber crisis management. It goes without saying that this kind of exchange of information will be a two-way street, and for the benefit of all those involved.
- **Between EU member states and other states where needed.** International cooperation (see Thematic Unit 3.14 – International Cooperation), presupposes the effective exchange of information, for the management

of incidents and crises that have an impact beyond one country. Any exchange should be based on anonymity and the protection of sensitive information, as appropriate.

In addition to the exchange of information on cyber threats and incidents, timely information on vulnerabilities in systems offered by the Cypriot market, in coordination with companies and customers (coordinated vulnerability disclosure), should be promoted.

The most appropriate form of cooperation will be explored to consolidate the exchange of information between stakeholders, and one possible form is that of public-private partnership. It is important to understand that there is a mutual benefit to such cooperation. It is recalled that for the most part, the private sector (including semi-public institutions) handles a large part of the critical infrastructure in Cyprus.

3.8.2. Situational Awareness

The term 'situational awareness', in relation to cybersecurity, refers to various levels of knowledge / understanding of the threat situation (i.e. in relation to threats related to systems and any attacks that may occur against the relevant systems). It also refers to the incident response capabilities of the various actors involved, related attacks that may occur in other countries, system vulnerabilities, as well as the level of implementation of technical and organisational measures (notably critical information infrastructures) appropriate to the level of risk.

Continuous and detailed mapping of the cybersecurity situation at national level requires close cooperation between the competent public sector authorities involved, such as the Digital Security Authority, the National CSIRTs, the Police, the National Guard (if needed), the intelligence services, other CSIRTs, other competent authorities (see section 2.3) etc. In any event, the contribution of critical information infrastructures is needed, depending on the situation. The collection and processing of information at central level (in the DSA), and its subsequent dissemination to any points deemed necessary, will optimize the benefit that will result from the implementation of the relevant actions.

This activity is directly linked to national risk management (see Thematic Unit 3.5 - Risk Assessment and Management – Criticality Assessment), even though its results will be more immediate and will reflect the situation at any time (real time situational awareness). A prerequisite is the creation of an efficient information exchange mechanism, without the implementation of which the success of this activity will be difficult. The successful implementation of Action 13 will help the competent authorities to achieve better levels of preparedness for cyber incidents and crises, with the consequent reduction of undesirable effects in the Republic of Cyprus.

Actions:

Action 12 – (a) Creation of the conditions and channels of cooperation and exchange of information cross-sectorally, between organizations, with the Digital Security Authority and where necessary, for more effective information and coordination regarding the response to threats and incidents in cyberspace (including: Information Sharing Analysis Centres - ISACs).

(b) Promoting the creation of a dynamic PPP in the area of information exchange, with the assistance of all critical information infrastructure stakeholders and competent state authorities.

Action 13 - Development of a holistic situational awareness mechanism, for the exchange of information and collaboration in real time, with the contribution of all involved bodies, including all competent authorities in the fields of cyber security, cybercrime, of cyber defence and international cooperation on related issues, and with centralized collection, processing and presentation of information, in order to increase levels of preparedness to deal with cyber incidents and crises.

3.9. Thematic Unit 9 – Awareness – Creation of a Security Culture

Strategic objectives: Education, Training and Awareness, Cooperation, Development of Capabilities

The range of potential cyber threats and risks, as mentioned in section 2.3, should concern all users of computer and communication infrastructures, networks, and terminal devices which are used by almost all citizens of the Republic of Cyprus, most of whom now make regular use of the Internet.

It is very important that Internet users, as well as users of computer and communication systems, in every workplace, are made aware and have a satisfactory level of knowledge about the potential cybersecurity threats from which they must be protected.

The competent authorities in the Republic of Cyprus should build on and expand the existing information programs currently implemented in Cyprus, the best practices for dealing with cyber challenges, as well as the activities promoted based on the existing Cybersecurity Strategy and in particular the National Cybersecurity Information Program approved by the Council of Ministers (for children, parents teachers and society in general). The extended information programme will contain (at least) the following:

- Creation of information material, as well as use of available material from external sources (e.g. ENISA, Safer Internet for Kids, etc.), for all citizens on issues of the safe use of the Internet, with the protection of personal data, proper behaviour in cyberspace and the protection of children on the Internet,
- Distribution of this information material using multiple means, e.g. TV, radio, SMS, websites, brochures/booklets, lectures, social media, etc.
- Creation of short-term training seminars aimed at employees,
- Creation of specialized seminars for civil servants and users of government information systems containing sensitive data,
- Promotion of the development of a 'security culture' in all government departments and agencies of the state, as well as in private enterprises.

As part of the implementation of the relevant corresponding Action in the previous Strategy, for the development of a culture of security, the development and approval by the Council of Ministers of the strategy for the safe use of the Internet for children, parents and teachers was promoted. The strategy covers a wide range of topics with the main objective of the creative and safe use of the Internet and new technologies. It promotes the development of knowledge and skills to exploit the potential of the Internet and new technologies as well as ways to meet the challenges arising from their use. In particular, it promotes the cultivation of a culture of security, and the development and application of horizontal skills - such as critical information management, responsible social behaviour, autonomous learning, communication and collaboration and problem solving. The strategy includes actions that concern children, as well as teachers, parents as well as the general public, and which aim to establish

a culture for the creative use of the internet with security and responsibility for a better internet for children and society at large.[16]

One of the actions resulting from this strategy concerns the creation of a "centre" (physical space and cooperation network) that promotes the safe use of digital technologies and especially the Internet. The creation of such a centre will have a great impact on the successful fulfilment of the purpose and objectives of this Cybersecurity Strategy, and in particular it can be a very important tool for the development of a culture of security and cybersecurity awareness. This activity emerged both from the suggestions of the stakeholders and from the analysis of the needs, views and suggestions of both children, teachers and parents as well as the entire Cypriot society. For the creation of the centre, a specific proposal was developed that was approved by the Council of Ministers while a more specific techno-economic study is being promoted that will allow the practical implementation of the "centre". The "centre" is expected to be exploited by various state services and institutions of the Cypriot society. The "Centre" will also play an important role in education and training issues referred to in Thematic Unit 10, as well as in research and innovation on cybersecurity and the use of new technologies referred to in Thematic Unit 11 - Research and Innovation and Thematic Unit 12 - Cooperation with the Private Sector.

Within this Action, emphasis will be placed and support will be given for the implementation of the specific strategy for children, parents and teachers, including the establishment and operation of the aforementioned centre.

In general, the formation of the appropriate cognitive level in the Republic of Cyprus, combined with the creation of specialized human resources for key positions in the field, in the long term will significantly contribute to the security of information systems connected to cyberspace.

Action:

Action 14 - Promotion and completion of the National Cybersecurity Awareness Program that will cover all users of electronic systems, from government and private employees, as well as the general public.
(a) The integrated Program will be developed in collaboration with all the involved agencies and interested parties regarding the issues of cyber security, with the aim of fully understanding the needs and the continuous improvement of the awareness levels and security culture regarding the cyberspace. The program will include awareness campaigns aimed at business executives and the general public.
(b) The implementation of the strategy for children, parents and teachers will also be promoted, as well as the creation and operation of the "centre" for the safe use of digital technologies and the Internet, with the goal of its use at the national as well as regional and European level. The coordinator of this action is the Pedagogical Institute of Cyprus on behalf of the Ministry of Education and Culture.

3.10. Thematic Unit 10 – Education and Training

Strategic objectives: Development of Capabilities, Education, Training and Awareness, Collaboration

This Thematic Unit focuses on activities related to promoting the development of capabilities in cybersecurity through the education and training of staff of government bodies, businesses and other organisations – which are vital for the state and to enable the development of the country's digital economy. This Thematic Unit connects and extends the objectives of Thematic Unit 9 beyond information issues to more specialized education and training. It is also linked to the capability-building topics of Thematic Unit 7 - Development of Capabilities - Organisation and

[16] https://www.esafecyprus.ac.cy/ethniki-stratigiki

Participation in Exercises, as well as to the research and innovation topics of Thematic Unit 11 - Research and Innovation.

In relation to this Thematic Unit, the strategy aims to facilitate the development of the curriculum to accelerate the development of cybersecurity skills across the education system. This includes the development of specialized learning and study programs in primary, secondary schools by incorporating relevant material on cybersecurity issues in all information and technology programs. It also includes the promotion and strengthening of relevant programs in higher education and the creation of special undergraduate and postgraduate programs on cybersecurity issues.

Appropriate cybersecurity training and capability building is a prerequisite for the smooth functioning of information security systems, as well as for the proper implementation of any actions in this regard. It is now a fact that, globally, there is a great shortage of properly trained cybersecurity professionals.

The development of the relevant capabilities is of major importance and the main objective of the Strategy is the creation of properly trained human resources, both in the public and private sector, who will have the necessary technical knowledge and experience to implement the provisions of the Strategy, as well as to contribute to the maximization of cybersecurity levels in Cyprus.

Therefore, the state should continuously support the appropriate training of personnel in the wide range of cybersecurity issues through, inter alia, the following actions:

- Identifying appropriate and available training programs and promoting certifications (national and international certification) for security professionals, based on the needs identified by government and industry;
- Promotion and exploitation of training programmes within the state, technical training should be complemented by initiatives focused on risk management;
- Creation of properly trained human resources with the necessary specialized knowledge, through the development of training programs in the field of cybersecurity and skills development for experts and non-specialists in both the public and private sectors;
- Integration of relevant certifications and experience into public sector service projects related to cybersecurity, and ensure career prospects for public sector staff specialising in cybersecurity issues;
- Promotion of school programs that raise students' awareness and encourage interest in network and information security issues and inform them about career opportunities in cybersecurity issues.
- Evaluation by the state of the possibility of creating various incentive programs, such as scholarships and/or grants for private education programs, as well as incentives to academic institutions to increase the number of graduates trained in cybersecurity issues;
- Promotion and support of the activity of higher and tertiary education schools in Cyprus in the field of network and information security and cybersecurity, through the integration of relevant topics in their programs.
- Addressing the gender gap in the education and training of cybersecurity experts, through a balanced approach that promotes, encourages and facilitates greater involvement of women in all efforts aimed at developing cybersecurity skills;
- Exploitation of the synergies that will be created with the establishment and operation of the "centre" for the safe use of digital technologies and especially the Internet mentioned in Thematic Unit 9 Information – Creation of a Security Culture and in Action 14(b).

It is emphasized that the emphasis in this Action is on training professionals in the field of cybersecurity and not on informing the public (see Thematic Unit 3.9 Information – Creation of a Culture of Security).

Action:

Action 15 - Development of appropriate human resources who will have the necessary technical knowledge and certifications for the proper implementation of the Strategy's provisions, in the medium and long term, and integration of this knowledge into the service plans for relevant jobs.

Promotion of actions for the appropriate education and training of personnel as recorded in this Thematic Unit 10.

3.11. Thematic Unit 11 – Research and Innovation

Strategic objectives: **Research and Innovation**

The speed with which the cyber environment is evolving today, and by extent the cybersecurity sector, demonstrates the great need to promote high-level research in this important field, as well as to support initiatives in the production of innovation. In order to be able to adequately address rapidly evolving cyber threats, a country must also be able to continuously develop its defence capabilities, and ensure that technologies and processes evolve at the same pace.

At an academic level, it is necessary to support and constantly update the educational programs offered by academic institutions through the conduct of high-level research. In addition, active in research activities (not only by academic institutions as well as by research institutions and companies active in the field), can receive funding from European and International organizations and programs, with the corresponding benefit to the national economy.

3.11.1. Promotion of Research and Innovation – Exploitation of funding opportunities

In this Thematic Unit, the strategy seeks to promote an environment that stimulates basic and applied cybersecurity research among critical sectors and different groups of stakeholders in order to support the strategy's objectives. The objectives of the strategy in this Thematic Unit, focus on the development of cybersecurity research and innovation programs in both state and private research organizations and academic institutions, and on the effective dissemination of new findings, technologies, processes and tools. It also seeks to establish links with the international research community in the scientific fields related to cybersecurity, such as, inter alia, computer science, artificial intelligence, electronic engineering, applied mathematics and cryptography, as well as in non-technical fields such as social and political sciences, business administration and psychology, etc. The strategy encourages the evaluation of mechanisms and incentives through grants, tax breaks, tenders and other initiatives that encourage the development of innovative cybersecurity-related solutions, products and services.

In order to achieve the objectives of this Strategy, the state has the will to dynamically promote research and innovation in the field of cybersecurity, with the main goal of meeting the needs and solving problems at national level as well as supporting European and international efforts for the development of the cybersecurity sector and the professional and scientific development of young scientists.

The further promotion of research and innovation in the field of Cybersecurity can be achieved through the cooperation of the private and public sector with local and international academic and other research institutions and organizations. This cooperation should be designed with a view to maximizing the benefit that Cyprus can derive by actively exploiting the various funding opportunities that exist, both at national level (e.g. through the new National Awareness and Education Centre of Excellence) and at European level (through funding programs such as CEF – Connecting Europe Facility, the ECSO – European Cyber Security Organisation, the Horizon 2020 Programme, SME – Small and Medium Enterprise research and innovation support, etc.), as well as at international level in the context of cooperation with international organizations such as. inter alia, the International Telecommunications Union (ITU) and the Organization for Security and Cooperation in Europe (OSCE), as well as attracting investment.

The state will support the efforts and initiatives by companies and academic and research institutions, to the maximum extent possible. Where possible, the Digital Security Authority will support and actively participate in co-funded projects, and will support domestic efforts to maximize the benefit for the Cypriot society and the exploitation of financing opportunities for the benefit of stakeholders and the economy.

3.11.2. Design and Development of Ecosystems

One of the main pillars of this Strategy, which is directly related to the promotion of research and innovation, is the design, development and creation of cybersecurity ecosystems. These cybersecurity activities are promoted for the first time in the Republic of Cyprus. The development of ecosystems has as its main objective to exploit the synergies created by exploiting the dominant position of Cyprus in sectors such as merchant shipping or in sectors where the country is a pioneer or has increased activity, such as financial services or energy, etc.

The development of cybersecurity ecosystems in critical sectors of the economy has as its main objective the upgrading of Cyprus' product, contributing to further the development of these sectors and in general to the upgrading of the cybersecurity situation in Cyprus. It also aims to assist European and international efforts to enhance cybersecurity in critical areas of international interest.

An important initiative promoted by the Digital Security Authority and supported by the competent authorities of the state concerns the creation of the "International Maritime Ecosystem for Cybersecurity". The Ecosystem concerns the provision of Cybersecurity services in the shipping sector at an international level. This is an innovative project of particular importance in the context of developing international and national security and economic stability. The proposed project is expected to upgrade the strategic role of the Republic of Cyprus at regional level, taking advantage of Cyprus' position in the field of international shipping. The 1st phase of the project concerns the conduct of studies in the framework of a co-funded project proposal submitted under the CEF Transport program of the European Commission. The 2nd phase of the project will focus on the operation and development of the ecosystem with the involvement of more stakeholders, competent authorities, organizations, system and service providers, shipping companies, etc.

In general, by investing in the design, operation and development of cybersecurity ecosystems, the state aims to better exploit the potential of the academic sector and businesses, to develop synergies with specialized activities of the state and to develop and specialize the capabilities of domestic human resources in critical sectors for the economy and society. These activities also aim to attract technology and cybersecurity companies and their activity in Cyprus, as well as to promote actions for the establishment and creation of innovative companies in the sector.

Actions:

Action 16 - Support and promotion of the production of research and innovation in the Republic of Cyprus in the field of cyber security. The research activities that will be promoted should be directly related to the needs identified within Cyprus as well as at the European and international level and should be able to support the objectives of this Strategy.

Action 17 - Assessment and creation of cyber security ecosystems in areas where the Republic of Cyprus is pioneering or showing increased activity, such as commercial shipping, financial services or energy and related activities. The ecosystems will be built on our experience as a country in these areas, with the support of the public sector, with the involvement of academic institutions and the private sector, and with the aim of attracting technology companies and organizations to Cyprus for the benefit of the economy, the state and of society.

3.12. Thematic Unit 12 – Cooperation with the Private Sector

Strategic objectives: Cooperation, Situational Awareness, Education, Training and Awareness, Development of capabilities

Given that cybersecurity is a significant challenge for the smooth and safe operation of the country's critical infrastructure, many of which are owned and / or managed by the private sector, cooperation with the private sector organizations involved is a necessity. Such infrastructure is found inter alia in the areas of energy, transport, health, water supply, banking and financial services. As we all know, security and risks are not only technological, technological solutions alone are not enough to protect the systems and operations of businesses and organizations. It should be ensured that there is sufficient awareness of the risks, as well as training and the acquisition of specialist knowledge by the executives of all organisations. The Digital Security Authority will actively contribute to the effort to train the agencies' dedicated staff on cybersecurity issues.

3.12.1. Establishment of a network of national contact points with the private sector

In the context of the implementation of the Strategy, the state comprehends and understands the dependencies that exist with the activities of the private sector, for the promotion and enhancement of cybersecurity. The aim of the strategy is to identify a network of authoritative national contact points for critical sectors and industries which are essential for the operation and restoration of critical services and infrastructure. These actions are also linked to the activities of Thematic Unit 1 for the creation of a Stakeholder Advisory Group, and the establishment of Sectoral Cooperation Groups. Within the framework of the structures that will be created, the role, involvement, commitments and responsibilities of all participants from the private and public sectors will be defined.

The network of national contact points with the private sector will act in consultation with the Commissioner and the DSA as well as with the state at large. Through the operation of the network, it will be possible to submit and discuss views and suggestions for the better implementation of the regulatory framework at sectoral and national level, as well as for the evaluation and treatment of more specific sectoral issues. It will also act as a means of exchanging information and best practices at sectoral and national level.

3.12.2. Establishing a formal public-private partnership (PPP – Public Private Partnership)

The strategy encourages the creation of a formal public-private partnership (PPP) to increase the security of essential services and critical information infrastructure. Public-private partnerships (PPPs) are the best means of effectively protecting critical infrastructure and managing security risks in both the short and long term. They are necessary to strengthen trust between them and between businesses, industry and government. However, the establishment of sustainable partnerships presupposes that all participants and stakeholders have a clear understanding of the objectives of the partnership and the security benefits resulting from the cooperation.

In the context of the specific cooperation between the state and the private sector, the establishment of a PPP (Public Private Partnership) in the field of protection of critical information infrastructures will be promoted, which will:

- contribute in building trust between the public and private sectors in network and information security issues;
- create a secure framework for cooperation to achieve common cybersecurity objectives;
- facilitate the exchange of information on new cyber threats and solutions to avoid them.
- support initiatives for the creation of Information Sharing Analysis Centres – ISACs, which are mentioned in Thematic Unit 8 and Activity 12(a).
- set up effective coordination structures and procedures and protocols for the exchange of information (see Thematic Unit 8 - Exchange of information), confidence-building, identification of points of improvement, and exchange of ideas, approaches and best practices to enhance security (see Thematic Unit 1 – Structures and Governance), as well as improving international coordination (see Thematic Unit 14 - International cooperation).

Action:

Action 18 - Horizontal action for the creation of PPPs in order to achieve individual objectives of the special actions such as innovation, information, education and training etc. as well as for the achievement of more specific objectives such as, inter alia, the creation of a platform for the exchange of techniques (and others , as the case may be) of information between the DSA and all those involved, in order to improve the levels of information for everyone and develop an environment of trust.
Other forms of cooperation that could be included in this effort will also be examined, such as e.g. participation in common systems and/or protection services against major attacks (Distributed Denial of Service - DDoS), etc., participation in common financial programs

3.13. Thematic Unit 13 – Security for All

Topics: Situational Awareness, Risk Management, Incident Management, Education, Training and Awareness

The strategy approaches cybersecurity issues holistically. In addition to the protection of the Essential Services of the Critical Information Infrastructures, Electronic Communications Providers, the State and the stakeholders from the private sector, small and medium-sized enterprises should also be taken into consideration and be supported by, and the citizens of the country. Raising awareness of cybersecurity threats and risks and their impact on society has become crucial. Through awareness-raising, citizens and corporate users can learn how to behave in the online world and protect themselves from standard risks.

Awareness-raising and information activities must be carried out on an ongoing basis and use a variety of delivery methods to reach a wide audience, as set out in detail in Thematic Unit 9 - Awareness and Creation of a Security Culture. In addition, all stakeholders and competent authorities such as the DSA, the National CSIRT, the cybercrime service of the Police, the Pedagogical Institute as the coordinator of the strategy for the security of children on the internet, internet service providers, as well as other involved parties shall inform the public on an ongoing basis about the dangers that occur and the precautions against malicious actions, mainly in relation to internet services. For this purpose, websites designed to provide information, support services such as the 1480 service (Cybersecurity helpline and Hotline), social media, applications on computers and smart mobile devices, etc. may be used.

In addition to the issues of awareness, education and training, the ultimate goal of the Strategy is the wider support of citizens in dealing with cybersecurity incidents with the active involvement of the National CSIRT. The implementation of actions such as the creation and operation of a help desk, staffed for instance with trainee staff and/or students could contribute in various ways to the provision of support to citizens as well as to the training of staff. An important mechanism for upgrading cybersecurity and developing the trust of society as a whole is the certification of products and services. This Strategy seeks to promote the implementation of appropriate certification schemes as approved in the EU Cybersecurity Act (EU Cybersecurity Certification Framework (EU))[17]. Through the relevant activities and actions of the Digital Security Authority, as the competent authority, emphasis should be placed on the certification of products and services through cooperation within the framework of the European mechanisms as well as the creation of appropriate national structures.

[17] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

3.13.1. Internet of Things (IoT)

In recent years, the Internet connects a huge number of users and connected devices – now there are refrigerators and other household appliances, cars, health devices, closed circuit cameras, telephones, intercoms, and even lamps, which have the ability to connect to the Internet. Internet of Things (IoT) devices are now found in most homes and are part of our daily lives, without necessarily adequately informing and raising the awareness of consumers about the dangers of malicious attacks through these devices. Such devices have been used in the recent past to carry out large-scale attacks (e.g. Distributed Denial of Service – DDoS) against various targets around the world.

At the same time, control systems and other devices which form part of critical industry infrastructure are now connected in most cases to the Internet. This is done for ease and flexibility in the use and management of such infrastructure. Due to the potential vulnerabilities of several of these systems, the consequences of any attacks are severe and can cause serious damage and even endanger human lives.

These systems and devices (IoT) can be categorized into four categories:

1. The device does not include any security provisions, usually due to its small size and minimal capabilities for functions beyond its basic functions. Furthermore, the devices usually still have the basic configuration given to them during their manufacture (default insecure configuration).
2. The device still does not include security provisions, but access to and from the device is controlled by an intermediate device (web service, gateway, etc.) which can protect the IoT device to a certain extent.
3. The device includes basic security functions independently, such as, for instance, integrity and confidentiality of communication.
4. Devices which incorporate security and protection measures at the time of their manufacture, to the level deemed necessary.

Unfortunately, it is observed that most IoT devices, on a global basis, remain at the first level of security, even though several efforts are being made by States, organizations or competent bodies to increase security levels for the benefit of users and other connected systems. In addition to the problems identified at the device level, there are other vulnerabilities related to all IoT devices within an organization (especially in industrial systems), such as inadequate guarding of basic security codes, enabled remote access, unpatched systems, unsecured protocols, etc.

In this Thematic Unit, issues related to the security of connected devices on the Internet of Things are expected to be studied. The main objective is to monitor the situation in relation to products which are widely available or widely used in the Cypriot market, and to issue guidelines for their proper use and the adoption of precautionary measures by users. The results of the work under this action could feed into the work that concerns the improvement of the legal and regulatory framework (see Thematic Unit 3 – Legal and Regulatory Framework) and the improvement of the security policies which will be assessed or covered in various other actions such as those concerning risk assessment, national cybersecurity framework, incident management, etc.).

Some basic principles concerning the security of devices and systems connected to the internet are set out below, which may be taken into account during the implementation of the relevant Action:

- integration of security practices and functions at the development and production stage of the products,
- integration of functions enabling the capability of retrieving forensic data,
- exchange of information on the security status of various devices placed on the market (see Thematic Unit 8 - Exchange of Information – Situational Awareness),
- obligations to enable remote security updates;
- promoting the building of trust and use of products that will be certified by European certification schemes (see EU Cybersecurity Certification Framework),
- authentication of devices from the networks to which they are connected,

- obligations for system hardening regarding systems which must have direct connections to industrial IoT systems, and
- other measures to be decided upon during the implementation of this Action.

3.13.2. Privacy and data protection

The cybersecurity strategy aims to take balanced measures for infrastructure and information security with privacy and personal data protection in mind. Balancing the two is a challenge since the implementation of the strategy's actions must take seriously into account the right to privacy of citizens. Privacy is a cross-cutting issue and is relevant to most of the activities mentioned in the strategy.

In this Thematic Unit, the main objective of the strategy is when defining any measures or actions to be taken into consideration, both security needs and safeguards to protect citizens' privacy and data. To this end, when planning more detailed actions:

- European and national legal requirements on data protection should be taken into account when preparing relevant cybersecurity regulations.
- the competent authority for the protection of personal data needs to be consulted on regulatory texts related to cybersecurity, where necessary.
- data protection law compliance measures should be considered during consultation in relation to minimum security measures unless they relate to national security issues.
- The DSA and the office of the Commissioner for the Protection of Personal Data should cooperate together where deemed necessary.

Actions:

Action 19 - Study and follow-up of the situation regarding the vulnerabilities and their rectification and in general the secure devices connected to the internet and falling under the category (IoT- Internet of Things), in the Republic of Cyprus, including industrial control systems located in critical industrial information infrastructures, and promote this action and the optimization of the legal and regulatory framework.

In due course, guidelines for the security of IoT devices and systems will be issued to organizations, companies and citizens, introducing specific obligations for entities that manage critical information infrastructures and operate industrial control systems.

Action 20 - Creation of national certification structures by the DSA in accordance with the EU Cybersecurity Act.

3.14. Thematic Unit 14 – International Cooperation

Strategic objectives: Cooperation, Incident and crisis management, Development of capabilities, Education, training and awareness

Cybersecurity plays role in many different areas of international relations, including human rights, economic development, trade, arms control, security, stability, peace and conflict resolution.

The strategy recognises that cybersecurity issues are not limited to the national level as well as the need to cooperate with other states, organisations and international factors. Problems and threats in the cyberspace cannot be adequately addressed by any country alone. International engagements with public and private factors are key to facilitating a constructive dialogue, developing trust and cooperation mechanisms, finding mutually acceptable solutions to common challenges and creating a global cybersecurity culture.

The state recognizes that issues of international cooperation on cybersecurity form an integral part of the country's foreign policy. To this end, the strategy encourages the development and use of skills focused on cyber issues (cyber-diplomacy), complementary to traditional methods and processes of diplomacy.

The implementation of the action foreseen by this thematic unit should set out the long-term objectives of international cooperation, identifying the competent authorities and organisations involved at national, European and international level.

The Republic of Cyprus has the will to participate in and support, inter alia, work on the establishment of international rules on cybersecurity and confidence-building measures, the development of cyber capabilities, and participation in the development of international standards in the field of cybersecurity. The efficient participation of Cyprus in European and international bodies presupposes the coordination of the various competent authorities at national level, so that the positions of the representatives of the Republic of Cyprus in the various bodies are harmonized and have been properly coordinated.

As far as external cooperation is concerned, at the present time, the Republic of Cyprus, through the relevant activities of the various competent authorities, is already represented in European bodies and relevant working groups as well as in international forums. An integral part of this Strategy is the continuous and constructive representation of the Republic of Cyprus in European and international bodies, aiming at the active participation and contribution of Cyprus to the work and important decisions of these bodies. Close ties with the respective competent bodies in other Member States of the European Union and international organizations should continue and should be strengthened with the aim of utilizing international cooperation for the continuous development and improvement of the strategic response of the Republic of Cyprus to cybersecurity issues.

At the same time, the participation and cooperation of the competent authorities of the Republic of Cyprus should continue in European actions aimed at improving the electronic security of European information infrastructures. It is noted that confidentiality must be taken into account when cooperating and exchanging information and experience with international bodies and working groups.

Action:

Action 21 - The interfaces and scope of cooperation with all parties involved within Cyprus will be strengthened, always on the basis of transparency and with the aim of achieving common goals for the benefit of the entire country. Furthermore, the good cooperation of the Republic of Cyprus with the other member states in the European Union, as well as third countries, will continue, through its representation and active participation in the relevant working groups and forums. This cooperation will support actions and measures at community level in order to improve cyber security throughout Europe and internationally.

3.15. Thematic Unit 15 – Tackling cybercrime

Strategic objectives: Cooperation, Reduction and effective investigation of cybercrime offences, Development of capabilities, Education, training and awareness

The rapid development of information technology has enabled the commission of a wide range of criminal offences using the internet and information systems and other electronic means, which require specialised investigation by law enforcement authorities. For this purpose, since 2007, the Office for Combating Electronic Crime and the Forensic Electronic Data Laboratory (OCEC & FEDL) have been established at the Police Headquarters.

The competent authorities face numerous and multidimensional challenges in the fight against child pornography, illegal access to computer data, racist comments via the Internet, financial fraud, extortion via the Internet, as well as other offences which constitute a crime under our national legislation.

The Republic of Cyprus has ratified the Budapest Convention on Cybercrime, as well as the Additional Protocol in order to enhance international cooperation and access to electronic evidence. At the same time, it recognizes the need to adopt legal rules for the preservation and acquisition of electronic evidence in criminal proceedings, as well as the monitoring of work carried out at European level.

Beyond the legal framework, there is a need to develop the capabilities of members of staff and to acquire appropriate means to fight cybercrime. To achieve this goal, the staff of the OCEC participates on an annual basis in special training programs. Therefore, the actions should take into account the working environment, the need to upgrade the workplace, the means of investigation of the OCEC & FEDL, as well as the training of staff.

Furthermore, the strategy takes into account that OCEC & FEDL is, among other services, responsible for informing the public about cybercrime prevention issues. In this area, targeted information of all organized groups is needed, as well as the preparation of timetables for the scheduled lectures that are expected to take place.

It also recognises that in the framework of cooperation, there is cooperation at national level with both the public and private sectors and at international level there is cooperation with Interpol, FBI, Council of Europe, Europol, CEPOL, Eurojust, ENISA and ENJ. Nevertheless, actions should focus on further strengthening cooperation with both the private sector (providers) in the investigation of criminal cases, and with Eurojust in the investigation of cross-border cybercrimes.

Actions:

Action 22 - Continuous monitoring and evaluation of the legal framework for the preservation and acquisition of electronic evidence in criminal proceedings at national and European level.

Action 23 - Development of capabilities of staff, upgrading the workplace, the means of investigation as well as the training of staff.

Action 24 - Targeted information of all organized groups for the purpose of preventing cybercrimes.

Action 25 - Strengthening cooperation between the public and private sectors during the investigation of criminal cases, as well as strengthening cooperation at international level in the investigation of cross-border crimes committed in cyberspace.

4 Strategy Management

The Strategic response of the Republic of Cyprus to the challenges posed by cyber risks and threats is achieved if the Actions are successfully implemented, if the networks and information used on a daily basis are protected, if any security incidents are properly handled and if cybercrime is addressed to the maximum extent possible, for the Cypriot Society as a whole.

4.1. Centralised Supervision and Management of the Strategy

For the purpose of monitoring the control of the implementation of the Strategy, an integrated (and unified) Program Management Plan will be developed, which will be the guide for the implementation of the Actions for a period of about four (4) years, and the means for the management of the Strategy as a whole. This document will cover a number of issues related to the Strategy, and will include (at least) the following:

- Cooperation interfaces and engagement of stakeholders with the creation of sectoral cooperation groups, where necessary (see section 3.1)
- Management of interdependencies between Actions (Interdependencies Management)
- Management and Optimization of Benefits
- Structured communications management, e.g. regular communication with stakeholders, dissemination of Strategy results, briefing of other bodies, etc.
- Creation of Key Performance Indicators (KPIs) to measure the results of the Actions
- Recording of targets for the desired level of cybersecurity of the Republic of Cyprus, with reference to the Cybersecurity Capacity Maturity Model for Nations[18] of the University of Oxford
- Risk Management in order to identify and manage any risks and conditions that could potentially adversely affect the execution of the Strategy and the success of its Actions
- Monitoring the results of the Actions and recording ways to improve future Strategies – lessons learned
- Promotion of the Strategy as a whole with a view to continuous improvement.

In order to provide better feedback on the effective implementation of the Strategy in the Republic of Cyprus, a biennial assessment of the maturity of the Cypriot society on Cybersecurity issues will be carried out every two years, such as the Cybersecurity Maturity Model implemented in Cyprus in the summer of 2017. The model was applied in relation to the results of the implementation of the first Cybersecurity Strategy of the Republic of Cyprus with a view to its revision by this strategy.

4.2. Management of Actions

The implementation of the individual Actions of the Strategy is a complex undertaking, because the issues are multidimensional and require the contribution of several stakeholders. These efforts will be more effective by adopting project management principles and procedures related to the implementation of each Action, making the implementation of the Strategy and all individual activities more effective. With the start of the implementation of the Actions of this Strategy, **work plans should be developed for each Action (where they do not already exist from the implementation phase of the previous strategy), with clear timelines, deliverables, costing and assessment of the necessary human resources to optimize the results.**

At the same time, it is recognized that the Actions included in this Strategy have common features and interdependencies between them. One Action may affect or feed results to another. There are also Actions with

[18] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm0

common goals, or which concern the same stakeholders. Therefore, a structured and holistic approach must be followed regarding the implementation of the Strategy as a whole, with a view to achieving the best results.

However, in order for each Action to be properly implemented, it must be analysed and expanded in detail, in order to identify all the actions that need to be taken. This will be followed by a detailed analysis and expansion of each Action of the response strategy, along with the identification of the resources and processes that will be needed in the context of its implementation.

As mentioned in section 4.1, a complete Program Management Plan will immediately ensue, which will also be the guide for the implementation of the Actions over a period of about 4 years. The time horizon of 4 years has been chosen to synchronise the implementation of the Strategy with the cycles of its main major activities (e.g. risk assessment at national level, exercises, regular cybersecurity level assessments, etc.).

In the context of the most detailed evaluation and analysis of the individual Actions, to the extent possible, the cost of implementation of each Action will be estimated as well as the time period during which the budget of relevant funds will be required, based on the detailed expansion of the Actions and actions that will be identified. This costing will be done in cooperation with the competent authorities, and in any case based on the importance of each Action and the scope of application, so that the costing is as realistic as possible for government services.

In parallel with the costing, the Actions described in this document will be prioritized, which will be evaluated (regardless of their costing), in terms of their significance and criticality in relation to the result they are expected to bring about for a safer electronic environment in the Republic of Cyprus. It is noted that this action will be completed regardless of the costing process of the Actions mentioned above. This prioritization will be included in the Program Management Plan, with an estimate of the implementation time of each Action within the overall four-year program.

In order to achieve an effective strategic response, its implementation should be regularly and rigorously evaluated. To this end, the results of the implementation of the measures and provisions contained in the relevant actions will be analysed qualitatively and quantitatively, as appropriate. A proper Cybersecurity Strategy should not be seen as a 'final plan', but instead its implementation should be closely monitored and reviewed at regular intervals. This review should take into account the results of the evaluation, as well as the new threats that appear (and will continue to appear) in cyberspace as well as any other new data that appear in this area.

The detailed expansion of the Strategy's Actions, as mentioned in chapter 3, will include indicators and evaluation criteria for each Action, where possible. The results of the evaluation will allow the proper revision of the Strategy with significant benefits to the Cypriot society.

ANNEX I - SUMMARY OF ACTIONS

Action 1 - Creation of appropriate structures and teams for the successful implementation of the Strategy, and to effectively deal with emerging threats in cyberspace, as well as emerging threats that will appear in the future. Where deemed necessary, the need to create new or to strengthen existing structures (e.g. sectorial CSIRTs) and partnerships will be studied, in order to maintain high levels of cyber security in the Republic of Cyprus. For all work that will be carried out within the framework of the Strategy, interdependencies will be taken into account wherever they occur… p.19

Action 2 – Creation of a mechanism for the coordination of Ministries, competent authorities and state services involved, on the basis of the structures which are mentioned in Thematic Unit 1, with the main aim, inter alia, of carrying out periodic meetings in which all interested parties will participate in order to inform them about action plans concerning state services, cooperation and coordination of actions… p.21

An example of a cooperation mechanism would be the creation of a dedicated working group to address a specific issue… p. 21

Action 3 - Full implementation of all provisions and regulatory framework of the NIS Directive, at all levels, with emphasis on critical information infrastructures and operators of essential services… p.22

Action 4 - Strengthening the existing legal, regulatory and regulatory framework for the full activation and support of the provisions of the Cybersecurity Strategy, and the creation of new legislation where necessary. All relevant legislation of the competent authorities should be examined if there is a need for adaptation. The legal framework for cooperation and information sharing with third countries and private sector organizations should be considered, as well as the promotion of a possible policy framework to incentivize businesses to upgrade and strengthen cybersecurity levels in their infrastructures. A process for monitoring the implementation and review of the legislation as well as compliance control mechanisms should be revised or established… p.22

Action 5 - Development of a National Cybersecurity Framework that will promote the protection of critical information infrastructures in the Republic of Cyprus, as well as of all government services of the state… p. 23

Action 6 - Assessment and management of cyber security risks in the Republic of Cyprus through a structured methodology to identify critical information infrastructures and the risks that may affect them, with an analysis of possible impacts and mitigation options (risk treatment options), as well as continuous improvement… p.25

6.1 The risk assessment will be carried out at regular intervals (every 2 years) to update the results and guide all the Actions of the Strategy, in accordance with the provisions of the NIS Directive and the existing national legislation… p.25

6.2 The criticality assessment will be carried out every two years and/or earlier if the need arises in accordance with the provisions of the NIS Directive and applicable national legislation… p.25

Action 7 - Development of a coherent methodology for risk assessment and management at the level of critical information infrastructures and essential services… p.25

Action 8 - Consolidation of the National (and other where appropriate - sectoral) CSIRTs in Cyprus, with the development of appropriate information exchange procedures and interfaces, in order to achieve effective incident response and management in the Republic of Cyprus… p.27

Action 9 - Development of an updated contingency plan to address cybersecurity crises and its use in all relevant exercises (link to action 11) … p.27

Action 10 - Development and promotion of measures, programs and activities to develop real cybersecurity capabilities in the organizations that manage critical information infrastructures, as well as in other organizations and companies, where necessary. These capabilities should cover the full range of cyber security activities - Identify, Detect, Protect, Respond, Recover in the context of continuous improvement… p. 29

Action 11- Planning and organizing regular national cyber security exercises, based on realistic scenarios, as well as active participation in Pan-European and other international exercises (link to Action 9) … p.29

Action 12 – (a) Creation of the conditions and channels of cooperation and exchange of information cross-sectorally, between organizations, with the Digital Security Authority and where necessary, for more effective information and coordination regarding the response to threats and incidents in cyberspace (including: Information Sharing Analysis Centres - ISACs) … p.30

(b) Promoting the creation of a dynamic PPP in the area of information exchange, with the assistance of all critical information infrastructure stakeholders and competent state authorities… p.30

Action 13 - Development of a holistic situational awareness mechanism, for the exchange of information and collaboration in real time, with the contribution of all involved bodies, including all competent authorities in the fields of cyber security, cybercrime, of cyber defence and international cooperation on related issues, and with centralized collection, processing and presentation of information, in order to increase levels of preparedness to deal with cyber incidents and crises… p.31

Action 14 - Promotion and completion of the National Cybersecurity Awareness Program that will cover all users of electronic systems, from government and private employees, as well as the general public… p.32

(a) The integrated Program will be developed in collaboration with all the involved agencies and interested parties regarding the issues of cyber security, with the aim of fully understanding the needs and the continuous improvement of the awareness levels and security culture regarding the cyberspace. The program will include awareness campaigns aimed at business executives and the general public… p.32

(b) The implementation of the strategy for children, parents and teachers will also be promoted, as well as the creation and operation of the "centre" for the safe use of digital technologies and the Internet, with the goal of its use at the national as well as regional and European level. The coordinator of this action is the Pedagogical Institute of Cyprus on behalf of the Ministry of Education and Culture… p.32

Action 15 - Development of appropriate human resources who will have the necessary technical knowledge and certifications for the proper implementation of the Strategy's provisions, in the medium and long term, and integration of this knowledge into the service plans for relevant jobs… p.33

Promotion of actions for the appropriate education and training of personnel as recorded in this Thematic Unit 10….p.33

Action 16 - Support and promotion of the production of research and innovation in the Republic of Cyprus in the field of cyber security. The research activities that will be promoted should be directly related to the needs identified within Cyprus as well as at the European and international level and should be able to support the objectives of this Strategy… p.35

Action 17 - Assessment and creation of cyber security ecosystems in areas where the Republic of Cyprus is pioneering or showing increased activity, such as commercial shipping, financial services or energy and related activities. The ecosystems will be built on our experience as a country in these areas, with the support of the public sector, with the involvement of academic institutions and the private sector, and with the aim of attracting technology companies and organizations to Cyprus for the benefit of the economy, the state and of society… p.35

Action 18 - Horizontal action for the creation of PPPs in order to achieve individual objectives of the special actions such as innovation, information, education and training etc. as well as for the achievement of more specific objectives such as, inter alia, the creation of a platform for the exchange of techniques (and others , as the case may be) of information between the DSA and all those involved, in order to improve the levels of information for everyone and develop an environment of trust… p.37

Other forms of cooperation that could be included in this effort will also be examined, such as e.g. participation in common systems and/or protection services against major attacks (Distributed Denial of Service - DDoS), etc., participation in common financial programs… p.37

Action 19 - Study and follow-up of the situation regarding the fixing of vulnerabilities and in general the secure devices connected to the internet and falling under the category (IoT- Internet of Things), in the Republic of Cyprus, including industrial control systems located in critical industrial information infrastructures, and feeding into the action and the optimization of the legal and regulatory framework… p.39

In due course, guidelines for the security of IoT devices and systems will be issued to organizations, companies and citizens, introducing specific obligations for entities that manage critical information infrastructures and operate industrial control systems… p.39

Action 20 - Creation of national certification structures by the DSA in accordance with the EU Cybersecurity Act… p.39

Action 21 - The interfaces and scope of cooperation with all parties involved within Cyprus will be strengthened, always on the basis of transparency and with the aim of achieving common goals for the benefit of the entire country. Furthermore, the good cooperation of the Republic of Cyprus with the other member states in the European Union, as well as third countries, will continue, through its representation and active participation in the relevant working groups and forums. This cooperation will support actions and measures at community level in order to improve cyber security throughout Europe and internationally… p.40

Action 22 - Continuous monitoring and evaluation of the legal framework for the preservation and acquisition of electronic evidence in criminal proceedings at national and European level… p. 41

Action 23 - Development of capabilities of staff, upgrading the workplace, the means of investigation as well as the training of staff… p. 41

Action 24 - Targeted information of all organized groups for the purpose of preventing cybercrimes… p. 41

Action 25 - Strengthening cooperation between the public and private sectors during the investigation of criminal cases, as well as strengthening cooperation at international level in the investigation of cross-border crimes committed in the cyberspace… p.41

ANNEX II - DEVELOPMENT OF CYBERSECURITY POLICY AND STRATEGY IN THE REPUBLIC OF CYPRUS –

HISTORICAL BACKGROUND

The Management of issues related to Network and Information Security and the coordination for the implementation of the Cybersecurity Strategy of the Republic of Cyprus was carried out until April 2018 by the OCECPR on the basis of Law 112(I)2004. The actions that preceded the current situation and the development of the second Cybersecurity Strategy of the Republic of Cyprus are briefly mentioned below:

1. On the basis of the competences stemming from Law 112(I)/2004 (sections 2(2)(g) and (j), 2(3), 18(3)(f), 19(1), 37(5), 39(2)(p), 42(7), 55(2)(b), 80(a), 97, 98) and the competence of the OCECPR to represent Cyprus in the Board of ENISA and to act as a central coordinating body in Cyprus between competent national authorities, the OCECPR had undertaken until now the coordination of the issues of security of electronic communications and information networks in the territory of the Republic of Cyprus and the coordination of the implementation of the Cybersecurity Strategy.

   Within the aforementioned framework, specific actions, measures and policies have been promoted over time and are being promoted at national level:

2. In 2006, the Ministry of Communications and Works (MCW) approved a policy document on the basis of which specific actions in the field of network and information security are promoted, through the OCECPR, including: the establishment of Emergency Response Teams for Network and Information Security Related Incidents[19] (CERTs/CSIRTs), the creation of an institutional framework for the security and integrity of infrastructure, as well as the provision of information to all affected persons and the wider Cypriot society on security issues.

3. In 2010, the MCW, following the suggestions of the OCECPR and the positive evaluations of ENISA, approved a detailed policy document for the commissioning of a Government and an Academic [20]CSIRT. Cyprus CSIRTs are built with the prospect of also covering the business sector at a second stage. The establishment of CSIRTs was institutionalised by a Decree of the CECPR, R.A.A. 358/2010 which was issued in August 2010.

4. In 2012, new provisions were introduced in the Electronic Communications and Postal Regulation Law, L. 112(I)2004, based on the new framework of the European Union in the field of Electronic Communications, concerning, inter alia, network and information security issues. The new provisions of the European framework have been implemented at European level since 25 May 2011.[21]

5. The aforementioned actions were adopted and complemented by the first Cybersecurity Strategy of the Republic of Cyprus, which was adopted by the Council of Ministers in February and entered into force in March 2013. This Strategy also covers horizontal issues and actions in the areas of cybercrime and cyber defence. It comprises 17 actions with technical, organisational and legislative measures, promotes awareness and training issues and strengthens cooperation between the public and private sectors. This document revises and modernises the Cybersecurity Strategy of the Republic of Cyprus.

[19] Policy paper on Network and Information Security 2006.

[20] Policy Document for the creation of Emergency Response Bodies for Network and IT Security Related Incidents and Incidents (CSIRT/CERT).

[21] Guidelines: "Better Regulation" Directive 2009/140/EC, and "Citizens' Rights" Directive 2009/136/EC.

ANNEX III - COMPETENT AUTHORITIES AND OBSERVERS IN THE REPUBLIC OF CYPRUS

In addition to the policy and actions mentioned in section 2.2, in the wider field of network and service security, information systems, as well as the information handled in them, other important actions are promoted by various authorities in the Republic of Cyprus that are directly or indirectly involved in critical security issues. Each authority has direct or indirect responsibilities in the field of network and information security, as well as interconnections and interdependencies between them, which must be taken seriously and which may substantially affect the implementation of this strategy.

The competent authorities of the Republic of Cyprus involved at this stage are the following:

- Deputy Ministry of Research, Innovation and Digital Policy (DMRIDP)
- Ministry of Justice and Public Order (MJPO)
- Ministry of Defence (MoD)
- Ministry of Foreign Affairs (MFA)
- Ministry of Finance
- Ministry of Education and Culture
- Ministry of Energy, Trade and Tourism
- Ministry of the Interior
- Digital Security Authority (DSA)
- Department of Information Technology Services (DITS)
- Cyprus Police (CP)
- National Guard General Staff (GEEF)
- National Security Authority (NSA)
- Cyprus Information Service (CIS)
- Office of the Commissioner for the Protection of Personal Data
- Department of Electronic Communications (DEC)
- Civil Defence (CD)
- Unit for Combating Money Laundering (MOKAS).

The authorities of the Republic of Cyprus which it is deemed appropriate at this stage to be kept informed (observers) are the following:

- Legal Services of the Republic
- Auditor General of the Republic
- Internal Audit Service
- Central Bank of Cyprus.

It is noted that the competent Authority of the Republic of Cyprus which is responsible for Classified Information (CI) and **European Union Classified Information (EU CI)** is the **National Security Authority.** Even though this document is not addressed solely or directly to the protection of Classified Information, the transmission of such information is essentially implemented through the communication infrastructure of the Providers of Electronic Communications.