Office of the Commissioner of Electronic Communications & Postal Regulation

Policy Document

Cybersecurity Strategy of the Republic of Cyprus

Network and Information Security and Protection of Critical Information Infrastructures

Version 1.0

23 April 2012

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Information and communications technologies and systems are one of the most important drivers of social and economical development today, whilst undoubtedly being necessary tools for the operation of functional and social structures in any country. As a result of this, a vital need is created for these technologies to offer ***security*** in their use, which is defined as the preservation of the principles of ***confidentiality, integrity and availability*** of information during its ***transmission, processing and storage.*** These principles lead to the building of ***trust*** in information systems and electronic services, which is considered a prerequisite for the continued development and growth in this valuable sector of the economy. ***Network and information security***, and more generally ***cybersecurity***, operates to maintain the above principles.

This Strategy aims to ***establish a safe electronic environment*** in the Republic of Cyprus, with specific considerations and actions for the ***protection of critical information infrastructures,*** whose disruption or destruction would have severe consequences to vital societal functions. The development and preparation of this Strategy has followed a ***holistic approach*** for responding to threats in cyberspace, recognising that a valid strategy must offer multiple levels of security.

The European Commission has set ***strong targets for the area of network and information security,*** which are evident from its intensified activities in this area, in cooperation with member states and with ENISA (European Network and Information Security Agency). The new European Regulatory Framework for Electronic Communications places special emphasis on the area of security and integrity of networks and services, and also on the area of ***protection of personal data.*** One of the main targets of the Commission is the ***development of National Strategies*** for network and information security (like this document), the ***development of National Contingency Plans*** for related matters and the ***creation of CERTs (Computer Emergency Response Teams)*** for incidents that involve electronic security breaches.

Even though the area of network and information security is not a new one, and there have been a number of related actions by various competent state authorities in the past, this document represents the ***first organised approach for coordinated response to threats that manifest in cyberspace,*** on a National level. The following priority areas have been identified to meet this target: ***coordination of the governmental stakeholders, development of a complete legal framework, technical and procedural measures, capability development and training, productive collaboration between the public and private sector and the creation or adaptation of the necessary structures and instruments within the Cyprus Government.*** This strategy document contains a series of actions that have been identified to achieve the goals discussed above, in the following areas:

- Organisational structures
- Legal Framework
- Collaboration between the public and private sectors
- Identification of Critical Information Infrastructures
- Threat landscape analysis

- National Cybersecurity Framework
- Incident response
- National and International Cyber Exercises
- Capability Development
- Awareness
- Cooperation with external agencies and international working groups
- Development of a National Contingency Plan for Critical Information Infrastructures
- Modelling and analysis of interdependencies.

Short summaries of the Actions, together with an initial graphical assessment of the interdependencies between them, are presented in Appendices I and II respectively.

This document also analyses the immediate actions that are to be taken within Phase A (see section 3.2), as well as the next steps that must follow, such as the detailed planning and costing for each action, the prioritisation and planning of the national cybersecurity programme, and the assessment of the results of the strategy actions that will follow. It should be noted that the ***Cybersecurity Strategy of the Republic of Cyprus will be reviewed on a regular basis*****,** taking into account the results of the assessment process, as well as new threats that appear (and will continue to appear) in cyberspace. The targets are to perform a holistic assessment of the results of the above actions and to update the strategy accordingly so that it continues to be in a position to provide the maximum benefit to Cypriot society.

1. INTRODUCTION

1.1 Network and Information Security

Information and communications technologies and systems are one of the most important drivers of social and economical development today, whilst undoubtedly being necessary tools for the operation of functional and social structures in any country. As cyberspace develops, the protection of the electronic systems present in organisations of all kinds becomes all the more important, so that any activity conducted through these systems is safe and secure. A basic security system must cover the confidentiality, integrity and high availability of infrastructure and information, while allowing the operation of the infrastructure to be reliable, flexible and controlled. Infrastructure security refers to the capability and resilience of the infrastructure against threats and malfunctions that may afflict its constituent parts. Relevant security measures that are taken mainly target the increase of readiness levels and the strengthening of preventative mechanisms, the identification and response to potential risks (including malicious actions or attacks), as well as putting in place measures for mitigation and recovery from malfunctions, failures and the availability of services that are offered, covering also emergency or crisis situations.

In this document, the terms ***'network and information security'*** and ***'cybersecurity'*** are used. 'Network and information security' refers to the preservation of the principles of confidentiality, integrity and availability, as they are described below. 'Cybersecurity' refers to the broader security of networked systems that operate in cyberspace, i.e. in most cases connected to the Internet, and this term also covers the safe and secure usage of these systems by end users.

It is clarified that the applicable level of information security must be guided through the determination of the ***value*** of the information to be protected (irrespective of the form of that information, whether it be physical or electronic). The value parameter will be taken into account during the implementation of the actions described in the present document, especially those that are related to informing people regarding security to foster awareness and a security culture. As a general principle, information must be protected appropriately, according to its value.

Network and Information Security is a basic and necessary consequence of the development and pervasiveness of new information and communication technologies. Taking into account the globalisation of communications, especially with the use of the Internet but also the continuously increasing dangers that users are faced with at all levels, it has become vital to take adequate protection measures but also to ensure a high level of cooperation between all parts of society, the public and private sectors, on a national, European and international level. Citizens, businesses and governments strongly need to be able to trust the media through which important information and data, personal or otherwise, is transmitted.

The safe development of information and communication technologies is important for citizens and societies, for growth in employment (and the economy in general), on the national but also the

European and international level. Investments in the area of security serve to increase the trust of users in new services and contribute to the wider development of the economy and society itself. Governments, as well as businesses, must evaluate their investments in this area, with the basic criterion being the costs associated with failures of their information technology or communication systems against malicious actions or natural causes.

'Security', in the information and communications technology world, generally refers to the preservation of three principles:

- **confidentiality** of information, i.e. to only allow access to information to authorised persons,
- **integrity** of information, i.e. the protection of information from any unwanted modification or destruction,
- **availability** of information or systems, i.e. for a system to be able to provide service and/or information when it is requested.

The preservation of the above principles aims to ensure network and information security to the highest possible degree, in relation to:

- the protection of information/data **in transit,**
- the protection of information/data **in processing,**
- the protection of information/data **in storage.**

Going beyond the protection of infrastructure, systems and information, the preservation of a high level of security, as per the principles described above, is necessary in order to built **trust** in information systems, communications and other electronic services that are offered by the government and other important organisations in Cyprus. The development of trust on behalf of citizens in these systems and ensuring secure transactions in cyberspace will contribute to a significant degree to the economic development of Cyprus and to meeting the targets of the Digital Agenda for Cyprus.

1.2 Critical Information Infrastructures

Information infrastructures have greatly increased in recent years in the Republic of Cyprus, and they have penetrated into almost every part of the life of the average citizen. These infrastructure are used not only directly (e.g. through the use of telephony, the Internet, etc.), but also indirectly, since almost all of the services that are offered by the government and used by citizens are heavily supported by them. Some of these information infrastructures form a critical part of Cypriot economy and society, either through the provision of vital goods and services, or forming a supporting platform for other (critical) infrastructures. These are thus considered to be *critical information infrastructures*, given that their disruption or destruction would have severe consequences to vital governmental and societal functions.

It thus becomes necessary, via a wider framework of a cybersecurity strategy of a country, to place special emphasis on the protection of such critical information infrastructures. A number of actions that are described in the present document cover the protection of critical information infrastructures, and

also the wider area of cybersecurity, given that these two areas are closely related and always interact with each other.

Section 3.6 describes, in further detail, the criteria that will be used to identify the critical information infrastructures in the Republic of Cyprus. The work that will follow for the development of a National Contingency Plan for critical information infrastructures is described in section 3.14 and forms a priority of this strategic plan.

1.3 Vision

The vision of the Cybersecurity Strategy of the Republic of Cyprus is the operation of information and communications technologies in Cyprus with the necessary levels of security, to the benefit of every user.

1.4 Aims and Objectives

The development of this strategy and the actions that have been identified have the following aims and objectives:

- the development and preservation of a safe and secure electronic business environment in Cyprus,
- support of the targets of the government that have been identified in the 'Digital Cyprus' strategy programme to develop conditions for an Information Society,
- the development of trust, on behalf of citizens and organisations/businesses, in e-government services, including the preservation of information and data in transit, processing and storage,
- the establishment of a safe electronic environment in the Republic of Cyprus for all of its citizens, including children,
- the mitigation of the effects of threats in cyberspace and the effective response to emergencies,
- the support of a future coordinated national response plan for the protection of critical infrastructures (beyond ICT) in the Republic of Cyprus.

1.5 Guiding Principles

The structure and contents of this document are based on the following guiding principles:

- the development of strategy and policy within a framework of cooperation between all competent authorities, taking into account the competences of each governmental stakeholder,
- the development of a holistic approach to face threats in cyberspace,
- the recognition that a valid strategy must offer multiple levels of security (layered security, defence in depth, etc.),
- the use of open processes in all stages of implementation of the Strategy,
- and the setting of ambitious goals with the will for the Strategy and its actions to contribute tangibly to the improvement of the levels of electronic security in Cyprus.

2. STRATEGIC CONTEXT

2.1 European Policy

Security matters form an important pillar of the Digital Agenda for Europe, and this specific European policy covers a number of important topics related to network and information security. The position of the European Commission regarding these issues is covered in detail in the strategy document for Network and Information Security (NIS). In addition to this, and as part of the application of European policy in this area, the European Network and Information Security Agency (ENISA) was created and has been operational since 2004. This organisation is headquartered in Herakleion, Crete and it develops pan-European and international actions in the area of network and information security, helping the application of European policy, the dissemination of information and best practices, the harmonisation and coordination of common actions, the organisation and execution of European and international cyber exercises and also international cooperation and coordination. The renewal of ENISA's operations (in time), with expanded terms of mandate, is the subject of intensive consultations during this period at the Council of Ministers level, and also in the European Parliament, given that everyone recognises the necessity of such an organisation to exist and operate in Europe.

The new European Regulatory Framework for Electronic Communications (with a May 2011 date of entry into force on a pan-European level), places special emphasis on the area of security, mainly in topics relating to: (a) the security and integrity of networks and services, as well as the application of regulatory measures and cooperation mechanisms on a national and pan-European level, together with national notification mechanisms for security breach incidents, contained in the Framework Directive (2002/21/EC, as amended), and (b) the security of personal data, the processing of such data and related security breaches, the protection of data contained within customer terminal equipment, and the use of automated calling systems and communication without human intervention, contained in the Directive on Privacy and Electronic Communications (2002/58/EC, as amended).

Additionally, cybersecurity matters have recently been placed high on the agenda of the Telecommunications Ministerial[1] Council of the European Union. The Council, during its recent meetings, has examined policy and the actions to follow, including the preparation of new Directives in the area of security and especially for Critical Information Infrastructure Protection (CIIP).

The Council has also requested the cooperation between Member States, the European Commission and third countries for: (a) the identification and securing of parts of critical infrastructure that could, if damaged or destroyed, have severe negative effects on member states, and (b) the exchange of information and best practices, while (c) urging member states to encourage effective cooperation between public and private sector entities, both within the member states themselves and with third

[1] The finalisation of the new European Strategy for Internet Security will form part of the activities of the Telecommunications Ministerial Council under the Cyprus Presidency of the Council.

countries. The Council has also asked to be updated, together with the European Parliament, on an annual basis by member states and the European Commission regarding their actions in these matters.

After the meeting of the Telecommunications Ministerial Council on the 27th of May 2011, in which these matters were discussed, the European Commission announced the actions that it expects the member states of the European Union to undertake, asking for the commitment of all those involved for the promotion of common goals. Specifically, the European Commission is requesting that member states and the Council state their strong commitment to the improvement and strengthening of national security in cyberspace to the best of their abilities, with the target of securing a high level of protection within the European Union and more effective collaboration on the international level.

As such, the European Commission is planning to monitor the performance of the member states closely, as regards meeting the three basic targets that are being promoted on the European level:

(a) The operation of national / governmental Computer Emergency Response Teams (CERTs) in each member state and the creation of a common and functional network of national / governmental CERTs in Europe by 2012, which will be supported by effective national cybersecurity strategies.

(b) The organisation of regular national and pan-European exercises for security in cyberspace (with CERTs participating as a prerequisite), in which a pan-European cyber exercise which has been scheduled for the second half of 2012 is included.

(c) The development of national contingency plans for network and information security, and incidents in cyberspace, and the contribution of all member states to the development of a European contingency plan for emergencies in cyberspace within 2012. Based on national experiences, such a plan must lay the foundation and define appropriate processes for effective communications between member states in situations where common threats and malicious attacks affect a number of member states.

On a national level, the actions described in points (b) and (c) above form part of the actions that are included in this Strategy. The action referred to in point (a) above is already in progress in the Republic of Cyprus and is regulated by separate secondary legislation that is published by the Commissioner for Electronic Communications and Postal Regulation, while the correct operation of CERTs/CSIRTs in Cyprus is a basic precondition for the development of the strategic planning that is described in this document. These same points were the subject of a special Ministerial Conference that took place in Hungary in April 2011, in the context of the work plans of the Presidency of the Council and of the European Commission during the first half of 2011. All member states were represented at this conference, which was under the auspices of the Telecommunications Ministerial Council and under the area of network and information security. The conference conclusions cover the duties of the member states in detail, as described in this section. Specifically regarding the matters related to CERTs, the conference conclusions state that:

«put in place well-functioning and operational national/governmental CERTs as soon as possible; provide technical support to the EU institutions in setting up their own CERT by 2012; establish a well-functioning network of CERTs at EU level, which will include the CERT for the EU institutions;».

In summary, the European Union, in recent years, has been planning, preparing and executing actions to strengthen its position in relation to cybersecurity. Its aim is to effectively handle the rapidly increasing rates of crimes and attacks in cyberspace, and the European Commission is asking from member state governments to seriously examine the issue of security in cyberspace.

The statement of Neelie Kroes, Vice-President of the European Commission for the Digital Agenda on the EU website is indicative:

"Cyber-attacks are a very real and ever-increasing threat. Whether against individual countries, companies or most recently against the European Commission, they can paralyse key infrastructure and cause huge long-term damage". She also added that: "Setting up this CERT pre-configuration team is a further demonstration of how seriously the EU Institutions take the cyber-security threat."

2.2 Network and Information Security in the Republic of Cyprus

The Republic of Cyprus and especially the Ministry of Communications and Works (MCW), and the competent coordinating authority[2] for Network and Information Security in Cyprus, which is the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR), have recognised the essential role of security topics in the promotion of new communications services, the use of new technologies and more generally in the development of an information society. Towards this end, a number of specific actions and policies have been promoted on the national level:

(a) In 2006, the Ministry of Communications and Works (MCW) approved a policy document[3], through which a number of specific actions in the area of network and information security are promoted, via OCECPR: the formation of Computer Emergency Response Teams (CERTs / CSIRTs), the creating of an institutional framework for the security and integrity of information infrastructures, and the raising of awareness of all stakeholders and Cypriot society about relevant security matters.

(b) In 2010, upon recommendations by OCECPR which were received favourably by ENISA, MCW also approved a detailed policy document[4] regarding the operation of a governmental and an academic CERT. The Cypriot CERTs are being formed with the extension potential to cover the private business sector at a later stage. The founding of the CERTs has been formalised via secondary legislation P.I.358/2010.

[2] Based on the provisions of the legislation that pervades its operations, OCECPR is responsible for the security of electronic communications infrastructures, as well as for the information that is transmitted through or stored within them.

[3] Policy Document on Network and Information security 2006

[4] Policy Document on the Formation of Emergency Response Teams for Incidents related to Network and Information Security (CSIRT/CERT) 2010

(c) Within 2012, new provisions are being introduced into The Regulation of Electronic Communications and Postal Services Law of 2004 (112(I)2004), which stem from the new Regulatory Framework for Electronic Communications[5] and which cover matters related to network and information security. These new provisions have been applied, on a European level, since 25th May 2011.

(d) The Republic of Cyprus, in cooperation with the relevant stakeholders, has committed, via the Telecommunications Ministerial Council, to contribute to European and international collaboration for responding to threats and challenges in cyberspace.

The National Cybersecurity Strategy that is described in this document adopts and complements the actions discussed above. Based on the provisions of this strategy and the priorities of the Republic of Cyprus, the actions related to network and information security form part of the wider strategy for the development of an Information Society[6], and will also allow for Cyprus to contribute actively in the planning process for protecting European critical information infrastructures from 2012 onwards.

2.3 Competent/Related Authorities and Observers of the Republic of Cyprus

Beyond the policies and actions that are mentioned in section 2.2, there are a number of authorities within the Republic of Cyprus that are active in the security of networks, services, information technology systems and information itself, in addition to having direct or indirect input on critical security matters. Each authority has direct or indirect responsibilities in the area of network and information security, as well as interdependencies between them that must be taken into account for the implementation of this strategy.

The competent/related authorities that are involved at this stage are the following:

- Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR)
- Department of Information Technology Services (DITS)
- Cyprus Police
- National Guard General Staff
- National Security Authority
- Central Intelligence Service
- Office of the Commissioner for Personal Data Protection
- Ministry of Communications and Works (MCW)
- Department of Electronic Communications (DEC)
- Civil Defence Force
- Cyprus Fire Service
- Unit for Combating Money Laundering

[5] "Better Regulation" Directive 2009/140/EC, και "Citizens' Rights" Directive 2009/136/EC
[6] See 'Digital Cyprus' document, as approved by the Council of Ministers in February 2012.

The following authorities of the Republic of Cyprus are to be kept informed of the activities described herein and are observers at this stage:

- Law Office of the Republic of Cyprus
- Auditor General
- Internal Audit Service
- Central Bank of Cyprus.

It is noted that the competent authority of the Republic of Cyprus that has responsibilities relating to **Classified Information (CI)** and **European Union Classified Information (EU CI)** is the **National Security Authority**. Even though this document is not aimed exclusively or directly at the protection of Classified Information, any electronic transmission of such information is essentially implemented through communications infrastructure of communications service providers.

2.4 Threats in Cyberspace Today

The use of computers and communications systems has nowadays penetrated our lives to a very high degree, and so our level of dependence on these technologies for much of our daily activity is increasing. These technologies are used today in many sectors beyond just for communications: they are used for the production and distribution of energy, the management of water and sewage systems, financial services, in the armed forces and law enforcement, governmental departments and services, health services, etc. Even though the benefits stemming from information and communications technologies (ICT) are huge, new network technologies have introduced a plethora of security issues that are taken advantage of by malicious actors that target vulnerabilities in infrastructure and network components, such as computers, routers, switches, etc.

The last few years have seen multiple threats appearing in communications networks, especially with the explosion in the use of the Internet by citizens. ICT has been used in malicious ways for theft from bank accounts, access to confidential information, damage to important websites (consequent denial of access to the public), etc. Examples of information that has been stolen from companies include confidential contracts, product designs, credit card information, account numbers and other personal data. Such incidents can induce severe damages to an organisation, given that its reputation and customer trust can be seriously affected, in addition to any direct (monetary) damages. The probability of such incidents occurring can however be significantly reduced if appropriate measures are taken by an organisation or enterprise.

It has been observed, on a global level, that not only is the frequency of attacks in cyberspace increasing, but also the complexity of such attacks. The public, in most cases, is not aware of the extent of these attacks, nor of the damages that can be caused by them. A relatively recent phenomenon that is being observed in cyberspace is that of *'botnets'* – automated virtual networks involving large numbers of computers (some have been reported with tens of thousands of 'members') that are controlled by malicious actors. These computers can be found in homes and businesses, and also

perhaps in governmental departments, without the users themselves being aware or having knowledge of this, and they are being used for large scale attacks in cyberspace.

In addition to the consequences to persons as described above, it is not difficult for problems to be created for nation states themselves. Interference with a nation state's communications has always been an inextricable part of military conflicts. Nowadays, given that many of an army's communications systems include computers, some nation states have already developed electronic weapons for attacks in cyberspace that can be used as part of a wider military offensive (or even for terrorist actions if they fall into the wrong hands). In addition to this, any vulnerabilities in the ICT systems of the armed forces could lead to the leak of very sensitive information to unauthorised users. The operations of modern military forces are dependent on ICT to a large extent and a serious cyber attack could have dramatic consequences to the defensive capabilities of a country. The strength, stability and safe operations of a country are now fully dependent on the smooth running of its infrastructures, and as can be seen from the examples mentioned above, cyber attacks cannot be ignored.

It is noted that the strategic response (see section 3) and the actions described in this document do not relate to the handling of military issues in network and information security, nor to the handling of related terrorism issues; however, the examples discussed above serve to highlight the level of dependence on the technologies that are discussed in this document that military networks and information have.

3. STRATEGIC RESPONSE

3.1 Priority Areas

The strategic response of the Republic of Cyprus to the previously mentioned threats can be split into a number of priority areas that have been identified for the optimal protection of critical information infrastructures. The areas that have been prioritised in relation to the needs of the Republic of Cyprus are the following, as shown in Figure 1:

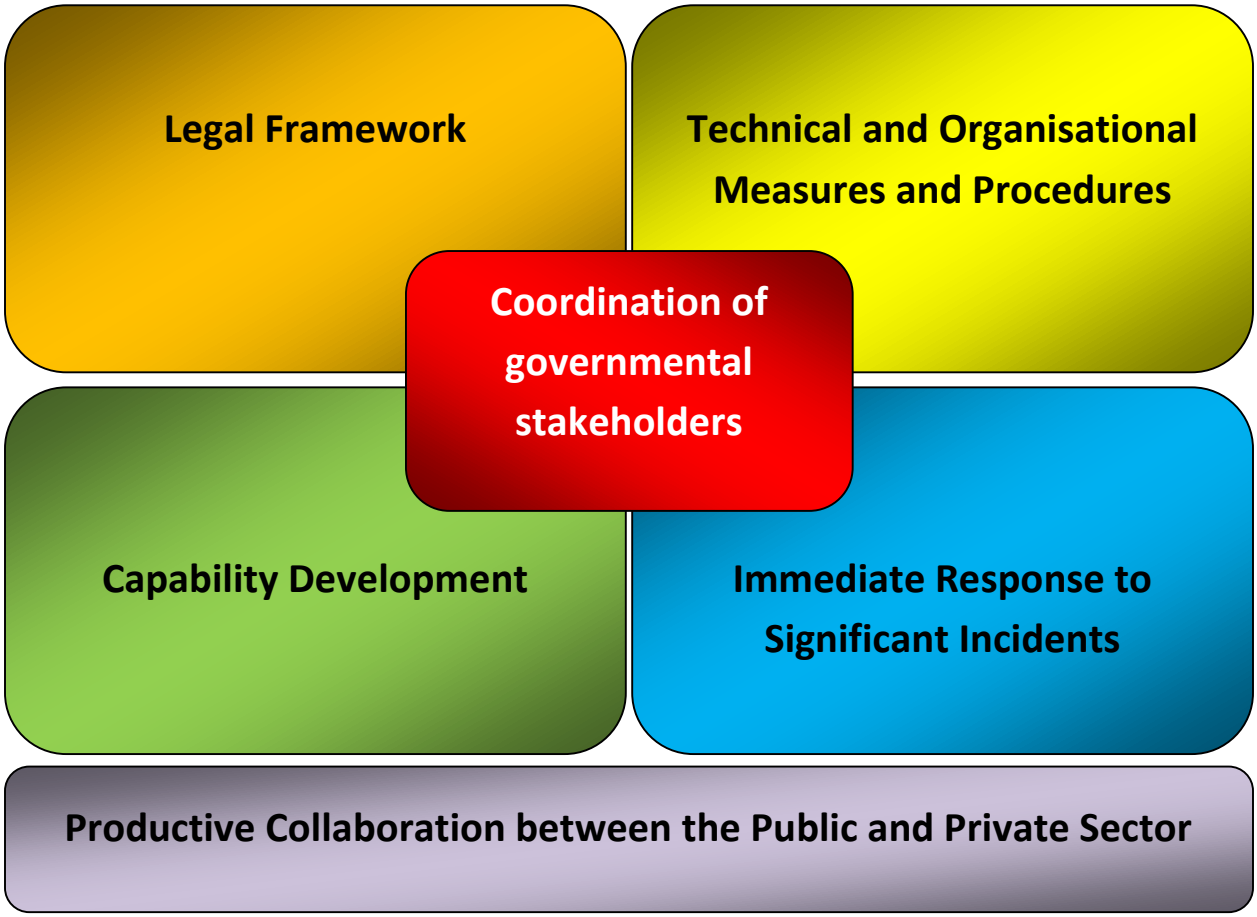

Figure 1: Priorities of the Cybersecurity Strategy of the Republic of Cyprus

- **coordination of governmental stakeholders** to ensure correct and efficient cooperation,
- **creation of a comprehensive legal framework** by the competent authorities of the state, that covers all aspects of network and information security, including cybercrime and the protection of personal data,
- **formulation of technical and organisational measures and procedures** to harden the security of relevant hardware, software and physical spaces, to the required degree,

- **development of the necessary skills, training and awareness** in security topics, for those that are directly involved and also for the public,
- **productive collaboration between the public and private sector**, on both the national and international level,
- **creation or adaptation of the necessary structures and instruments** within the competent authorities and the more generally the Cyprus Government, to secure the demands and capabilities of immediate incident response.

3.2 Splitting the Actions – Phases A and B

The rest of this chapter presents the actions that have been identified for the implementation of the strategic plan. Current organisational structures and available resources are not at a level that would allow an immediate start to all of the actions that have been identified, and as such each action description that follows also indicates the phase in which it will be executed:

- **Phase A**
  - Phase A includes all of the actions that OCECPR is in a position to start in the immediate future with the resources that are currently available to it.
- **Phase B**
  - Phase B includes the actions that OCECPR will be in a position to coordinate once a new organisational structure has been developed, with the necessary resources to carry out the implementation of this Strategy in its entirety.

Each action description mentions the phase in which it will be executed and the actions that mention both phases will be partly completed in each phase. It is noted that this does not mean that actions implemented in Phase A will necessarily be completed within that phase. The majority of the actions of this Strategy will continue to be executed on a long-term basis for the continued protection of cyberspace in Cyprus.

3.3 Organisational Structure

The area of network and information security is a very large and complicated subject, and one which involves a number of stakeholders, as shown in section 2.3. Each competent or relevant authority has its own areas of responsibility and it is important to uphold these differences. However, due to this multi-stakeholder approach to security matters, it is vital for all involved to understand and accept that the maintenance of acceptable levels of security in the electronic world can be accomplished **only** via cooperation between the different stakeholders involved, within a framework of coordinated response to the various threats that have already been mentioned.

It follows that the coordination of the competent or relevant governmental authorities is absolutely necessary. This coordination activity is productive when performed by an entity which is in a position to organise and coordinate the various actions of the Republic of Cyprus for correct response to the threats that are around today, as well as rising and new threats in cyberspace. This entity must have:

- the **appropriate legal authority and defined responsibility** in order to carry out its duties,
- the **necessary skills and capabilities** to respond appropriately to the obligations of the role,
- the **necessary links and good working relationships** with the competent or relevant authorities of the Republic, the electronic communications providers in Cyprus, the private sector stakeholders and international working groups and fora that are relevant to the area of cybersecurity.

Taking into account the fact that the definition and creating of an integrated and complete organisational structure is necessary for the optimum implementation of the strategic actions, but also that the processes involved to accomplish this are affected by external factors related to the current severe financial crisis that is manifesting in Cyprus, and the lengthy recruitment procedures involved, the implementation of such an organisational structure will form part of Phase B of the strategy activities. This will have the following benefits:

- The planning and executing of the actions that have been identified as being of an urgent nature and with immediate priority, for which the legal framework is already in place, will not be delayed.
- Existing structures will be leveraged to the maximum extent possible, with gradual upgrading of their capabilities to the required level.
- The associated financial burden will be gradual and in line with the capabilities of the Cyprus economy.
- Cypriot authorities will be in a position to fulfil their commitments both on the national and European level, where relevant activities are being pushed forward with rapid and demanding timelines.
- The necessary time will be given for the appropriate needs assessment, in relation to the requirements for the strategy implementation, the coordination of activities and the supervision of incident response mechanisms and related actions.

Phase A will formulate the cooperation framework between OCECPR, as the coordinating body, and the other competent authorities for the implementation of the high priority actions, such as developing the plan for the protection of critical information infrastructures, the operation of the governmental CSIRT/CERT, the assessment and improvement of the readiness levels of network infrastructures as regards their resilience to risk and their response to security threats, the handling and notification of security incidents on networks, systems and information, and the organisation of national exercises with additional participation in European exercises. These activities refer to the wider responsibilities that OCECPR has in the area of network and information security, and section 2.2 discusses the specific actions that have been prioritised and have been included in this strategy. At this point, an agreed basis for cooperation is required between the competent authorities, and which will be expanded and adjusted as the strategy programme progresses.

Action 1 - Phase A – Formulation of the framework for collaboration and information exchange with OCECPR, and between public authorities, so that OCECPR will be in a position to effectively coordinate the nation's strategic response in the area of cybersecurity and the protection of critical information infrastructures, as well as coordinating the actions that relate to other stakeholders in the priority areas that can be addressed immediately.

The way that existing activities in the area of network and information security, that fall under the responsibilities of OCECPR, are planned and executed is based on its existing organisational structure. The present structure and resources are not adequate to take on and execute all of the actions that are described in this document. As a result of this, and in tandem with pushing forward with the immediate priorities based on current urgent national and European commitments and needs of the Republic of Cyprus, OCECPR, in cooperation with the other competent authorities in the Republic, will study and submit recommendations regarding new policy for its reorganisation to the Minister of Communications and Works, so that it will be in a position to fully coordinate the very large volume of work associated with the areas of network and information security and cybersecurity.

Action 2 - Phase A – OCECPR will, at the appropriate time and in cooperation with the other competent authorities, develop a report regarding new policy for its reorganisation, so that it will be in a position to fully coordinate the efforts of the Republic of Cyprus for optimum implementation, application and supervision of all of the actions and the effective response to threats that are prevalent in cyberspace today, as well as rising threats that will appear in the future.

OCECPR will also coordinate the formation of a number of working groups, which will take over the implementation of the rest of the actions that are described herein. These working groups will be staffed by personnel with the necessary technical and other skills from the competent authorities of the state, as well as by experts from the private sector and representatives of critical information infrastructure operators (see also section 3.5).

For the identification and assessment of potential risks, it may be the case that the members of some of the working groups might need access to classified information; that is the information that refers to vulnerabilities in critical parts of each network or system that will be deemed as important or critical. Taking into account that the relevant risk assessments must be conducted in tandem with the development of plans to respond to incidents relating to these risks, and also the development of contingency plans to mitigate the effects of related disasters, the composition of the working groups must be such that confidentiality is assured.

Action 3 - Phase A/B – Formation of working groups, with representatives from the public and private sectors (as necessary), to implement the Strategy Actions.

3.4 Legal Framework

Legislation in the Republic of Cyprus already covers a large number of areas relating to network and information security, as well as cybercrime (and other electronic crime) matters. However, it is still considered necessary to identify **all** relevant laws in Cyprus and to update them where needed, and also to promote the creation of new primary and secondary legislation to cover all of the provisions of this Strategy. This legislation (whether new or updated) must cover processes for the prevention, deterrence and dynamic response to all forms of cybercrime, and also be harmonised with the relevant law and directives of the European Union.

International cooperation with other member states of the European Union, as well as third countries, will be required in the areas of network and information security and the protection of critical information infrastructures. As such, specific legal issues may arise regarding the processing and handling of electronic threats whose sources could be outside of the boundaries of the Republic of Cyprus. It is thus considered necessary to create an appropriate legal infrastructure also regarding the effective cooperation with entities outside Cyprus to solve related problems as they arise.

Action 4 - Phase B – Creation of an appropriate legal framework to fully support the provisions of the Cybersecurity Strategy. All relevant laws of the competent authorities must be assessed for any updated needs.

3.5 Cooperation between the State and the Private Sector

The State will make significant efforts in the area of network and information security, and especially on the topic of critical information infrastructure protection within Cyprus. The strategic initiative in these areas can only come from the State, which is responsible for ensuring the cooperation between relevant stakeholders on a national and international level.

The State recognises that the **role of the private sector** in the security and protection of critical information infrastructures **is extremely important**, for the following reasons:

- The private sector (including the semi-governmental electronic communications provider) operates the majority of the critical communications infrastructure of the government, e.g. the

public communications networks that are used by the different government departments, as well as by the business and academic worlds, and the citizens of the Republic.

- The State relies on the private sector, not only for the communications networks, but also for the provision of the equipment that it uses, and for the implementation of many of activities that are related to network and information security, whether those are conducted as a matter of course for security reasons or for the reliable operation of their systems and services, or they are imposed on the operators via legal and / or regulatory measures.
- It is considered a given that the private sector contains accumulated technical know-how and specialised human resources, and there are also organisations that can help and contribute to the best possible development of the Republic of Cyprus in these areas.

Taking the above into consideration, the Republic of Cyprus sets a high priority on consultation with the private sector for the achievement of its goals, the implementation of the provisions of this Strategy, the continuous improvement of the actions and effects of the Strategy, as well as for the gaining of further technical skills and specialisation.

Action 5 - Phase A/B – Comprehensive survey of the private sector, for the identification of groups and stakeholders that can contribute in a positive way to the improvement of the levels of electronic security in the Republic of Cyprus, while simultaneously creating the conditions for developing close collaborative relationships.

During the execution of the Action described above, the State will seek out cooperation with existing competent authorities which determine the way that important sectors operate, such as the Central Bank of Cyprus regarding the banking sector. In addition to this, a mechanism for providing regular updates to the private sector will be put in place, regarding the progress being made in the planned actions, to help achieve convergence in the activities of the public and private sectors regarding the provisions of this Strategy.

Beyond what has been described above, the PPP (Public-Private Partnership) model is emphasised, which is considered on a European and international level to be an effective model of cooperation between entities in the public and private sectors. With the requisite preparatory work, the possibility of creating a dynamic PPP in the area of critical information infrastructure protection will be investigated, and which will:

- **contribute to the development of trust between the public and private sectors in the area of network and information security,**
- create a safe cooperation framework to achieve common security goals,
- facilitate the exchange of information related to new threats in cyberspace and solutions for their avoidance,
- allow cooperation in research and innovation in related topics,

- help to set ambitious but feasible targets for the realising the vision of the Strategy,
- cooperate with PPPs in other member states of the European Union in the same area, via active participation in related working groups.

Action 6 - Phase B – Investigate the possibility of creating a dynamic PPP (Public-Private Partnership) in the area of critical information infrastructure protection in the Republic of Cyprus and promote active cooperation with international entities through participation in international fora. The use of the PPP to foster trust between the State and private sector will be of primary importance.

3.6 Identification of Critical Information Infrastructures

The need for the protection of critical information infrastructures, as highlighted and explained in this document, is necessary to minimize the negative impacts and possible catastrophic consequences of malicious acts or natural disasters on infrastructure, on a national level within the Republic of Cyprus but also because of potential negative effects to other countries, as a consequence of the high levels of interconnection and interdependence between international communications networks. The question is raised as to which particular infrastructures should be considered (and designated) as 'critical'. Each stakeholder (electronic communications companies, governmental departments and services, security forces, armed forces, hospitals, financial institutions, energy and water providers, etc.) will consider their infrastructure as vitally important and the ideal situation *would be* the complete and total protection of all information infrastructures in the Republic of Cyprus, without exception.

However, given that such an approach is not feasible, it is necessary to identify and assess the truly *critical* infrastructures within the Republic of Cyprus and to target them for the best possible protection. These critical infrastructures will be identified and assessed based on a number of predetermined criteria. For the determination of these criteria, as well as national conditions, related activities of the European Commission and ENISA (European Network and Information Security Agency) will also be taken into consideration, with the appropriate adaptation for Cyprus. The public sector, as well as the private sector, must contribute to the determination and assessment of critical information infrastructures, within the boundaries of the relevant working group(s).

The steps that will be followed for the identification of critical information infrastructures will include the following:

- **Determination of services** that will be targeted (e.g. voice communications, data communications, data storage, data processing), that could be classed as critical,
- **Identification of infrastructures** that are technically indispensable for the operation of these services,
- **Introduction of objective criteria** for the level of protection that each infrastructure element needs, with categorisation of infrastructures and the use of criteria such as the number of

affected users, the sensitivity level of the information that is concentrated, stored, transmitted or processed on these infrastructures, etc.

- **check the criteria** with the development of scenarios that consider the disruption of operation of selected infrastructure, within the bounds of regular exercises.

Action 7 - Phase A – Identification and assessment of the critical information infrastructures in the republic of Cyprus, to better target activities and actions for their protection, with the contribution of both the public and private sectors.

3.7 Threat Landscape Analysis

Section 2.4 mentioned the general threats that can manifest in cyberspace. It is important to note that available information on the specific mix of threats that appear in Cyprus and which can rise in the future is limited. The protection of information infrastructures can be achieved through general measures only (to some extent), but the strategic response to threats in cyberspace will be greatly improved if the main threats that are actually present and manifest in Cyprus become known. This will not only allow better targeting of response measures, but also better targeting of the most prevalent threats if the necessary protective controls are put in place gradually through a feasible implementation programme for the provisions of this Strategy.

A comprehensive threat landscape and attack analysis is therefore necessary (including attacks that are widespread in Cyprus and other European countries), so that the improved targeting of response methods can be achieved, as discussed above. This analysis will be combined with the most prevalent threats that are discussed in European and other international reports for a more complete and comprehensive review.

Action 8 - Phase B – Comprehensive survey to record current threats and attacks in cyberspace that have been published in Cyprus, as well as monitoring new threats that appear in the European and international space.

3.8 National Cybersecurity Framework

The easiest and most effective method to achieve an acceptable level of security in all critical information infrastructures in the Republic of Cyprus is to develop a National Cybersecurity Framework, which will be used as the basis for the protection of critical information infrastructures, and for information assurance. This framework must be developed based on international security standards and include the following (among others):

- Governance and risk management
- Vulnerability assessment
- Regular penetration testing
- Management of physical spaces, hardware and software
- Appropriate staff authorisation
- Physical security and environmental management
- Making use of CERTs for incident management (see section 3.9)
- Continuous monitoring of electronic communications for malicious attacks to determine incidents in progress.

This Framework must be adopted by all operators of critical information infrastructures, and must also be examined for adoption by all government departments and other important organisations in Cyprus. To achieve this target, the National Cybersecurity Framework will be developed in such a way so that it can be promoted within the remainder of the private sector, for the optimum protection of all those that use electronic communications services.

Action 9 - Phase B – Development of a National Cybersecurity Framework which will promote the protection of critical information infrastructures in the Republic of Cyprus, as well as governmental departments and services.

It should be noted that the specific targets that will be set for the protection levels for these technologies and systems will be determined based on appropriate risk analysis and balancing these levels with the associated cost of implementing specific controls to respond to threats in cyberspace. A usual method used is to keep the related annual costs below the annual estimated cost of damages or losses if these threats were to manifest on information and communications networks and systems.

3.9 Incident Response

Ensuring the full functionality of Computer Emergency Response Teams (CERTs/CSIRTs) within Cyprus is an integral and vital part of this Strategy, and also of meeting our commitments as a nation.

The main functions of a CERT are the prevention of serious incidents related to network and information security, as well as the immediate and appropriate response to such incidents when they occur. It is emphasised that for the correct operation of a CERT/CSIRT, the following are required: (a) necessary infrastructure and (b) staffing with appropriately trained (to a very high level) personnel. A basic prerequisite for such services to operate effectively is strong support from the State.

The cooperation between CERTs/CSIRTs that operate in each member state lies within the framework of European cooperation in the area of information security. Given the target of integrating Cypriot

CERTs/CSIRTs into these cooperation mechanisms, their full functionality must be ensured so that they may gain the necessary certifications to allow their participated in relevant European working groups.

Action 10 - Phase A – Ensure the full functionality of Computer Emergency Response Teams (CERTs/CSIRTs), with immediate priority for the operation of the Governments CERT/CSIRT. Necessary certifications and memberships will be obtained to allow their participation in relevant European working groups.

Action 11 - Phase B – Assessment by OCECPR, in cooperation with the CERTs/CSIRTs, of expanding their activities or creating new CERTs/CSIRTs to cover the needs of the private sector and the business community.

3.10 National and International Cyber Exercises

The significant need for cooperation between the government and different stakeholders, both within the public and private sectors, has been examined in sections 3.3 and 3.5. The development of this cooperation, and especially of associated trust, is of the utmost importance.

However, it is not enough to just create the necessary cooperation mechanisms, if these mechanisms are not assessed and tested on a regular basis, especially via the emulation of crisis situations. The completion of such exercises has proven to be a very valuable tool for ensuring the readiness levels of the competent authorities to handle a potential crisis, e.g. the loss of a significant part of a large communications network. Exercises that have been conducted so far in other member states, and also on a pan-European level, have shown that the mechanisms to face such a crisis already exist; the missing piece of the puzzle is usually the **cooperation and coordination modalities** between the competent authorities involved, i.e. who will communicate with whom in a crisis situation, how can rapid cooperation between the involved authorities specifically be achieved, etc.

The need for completing cyber exercises that involve handling realistic scenarios (where the players involved have no *a priori* knowledge of the events that are to follow) has been recognised on the European level and the first pan-European cyber exercise (Cyber Europe 2010) has already taken place. The Republic of Cyprus has much to gain for organising and actively participating in such cyber exercises. Naturally, this gain is maximised with the organisation of similar national exercises with realistic scenarios. The completing of such exercises will contribute to the maximisation of the Republic's readiness levels to withstand significant events in the area of network and information security that could potentially affect a large part of the population.

It is noted that the element of confidentiality must be taken into account during all cooperation and exchange of information and experiences with international organisations and working groups, as described in section 3.3 regarding the formation of the working groups.

Action 12 - Phase A – Planning and organisation of regular national cybersecurity exercises, with increasingly realistic scenarios, as well as active participation in pan-European and other international cyber exercises.

3.11 Training and Capability Development

The appropriate technical training and development of capabilities in the cyberspace security area is a necessary prerequisite for the smooth operation of security systems, as well as for the correct implementation of any actions related to this theme. The development of such capabilities is of major importance and the target is to create a suitable workforce, both within and outside of the public sector, which will have the necessary technical know-how and experience to implement the provisions of this Strategy.

As such, the government will support the appropriate personnel training in the area of electronic security, via the following actions:

- Identification of appropriate (and available) training programmes and certifications,
- Promote the uptake of such programmes within the government,
- Creation of a suitable workforce with the necessary specialised knowledge,
- Inclusion of relevant certifications and experience into job descriptions that relate to electronic security,
- Support activities in Cypriot higher education institutions in the area of network and information security, through the inclusion of electronic security topics in their curricula and the institution of related research programmes.

It is noted that this action refers to the education and training of professionals in the area of cybersecurity and not in awareness raising measures for the public (see section 3.12).

Action 13 - Phase B – Development of suitable human resources that will have the necessary technical know-how and certifications to implement the provisions of this Strategy to a high level, in the mid- and long-term, and inclusion of these skills and certifications into the job descriptions for related positions.

3.12 Security Culture (Awareness)

The dimensions of potential threats to cybersecurity, as discussed in section 2.4, clearly show that this issue concerns **all** users of information infrastructures, given that any connected computer could serve as an entry point or malicious and/or harmful elements to local cyberspace. This includes the vast majority of the citizens of the Republic of Cyprus, given that most of them today makes use of the Internet on a regular basis.

It is very important for Internet users, as well as users of IT systems in every workplace have a satisfactory level of knowledge/awareness regarding the potential threats that they must protect themselves from.

The Republic of Cyprus will promote a National Awareness Programme for cybersecurity matters, which will include the following:

- Creation of informational material, as well as use of existing (and available) material from external sources (e.g. ENISA), for citizens regarding safe and secure Internet use, with a focus on the protection of personal data, ethical behaviour in cyberspace and protection of children on the Internet,
- Distribution of this informational material through multiple media, e.g. television, radio, SMS, websites, leaflets/booklets, lectures, etc.
- Development of small duration training seminars for working professionals,
- Development of specialised training seminars for governmental users of IT systems that contain sensitive and/or classified information,
- Promotion of the development of a positive security culture in all government departments and services, as well as in private businesses.

Action 14 - Phase B – Development of a comprehensive National Awareness Programme for cybersecurity matters, covering all users of electronic systems, from governmental workers to citizens of the State.

Reaching the appropriate level of knowledge and awareness in Cyprus, combined with the development of skilled human resources for key positions, will contribute significantly in the long run to securing IT systems that are part of cyberspace.

3.13 Cooperation with External Agencies and International Working Groups

As has been discussed extensively previously in section 3.5, cooperation of the main body responsible for ensuring the security of cyberspace in the Republic of Cyprus with other stakeholders is not merely a

choice, but has become absolutely necessary to achieve the required targets and results. Problems and threats in cyberspace cannot be fully mitigated by a single country alone, and as such, constructive cooperation between states on the European level is required.

The Republic of Cyprus, through the activities of OCECPR and of the other competent authorities, is already represented to a high degree at most relevant working groups and international fora which operate under the auspices of the European Commission and of ENISA. The continued representation of the Republic of Cyprus at such fora and working groups is an integral part of this Strategy, with the target of **active participation and contribution** of Cyprus to significant decisions that are made via the work of these groups. Close ties will be created with respective competent authorities in other member states of the European Union, and these ties will be leveraged for the continuous development and improvement of the strategic response capabilities of the Republic of Cyprus in cybersecurity.

Full support of actions and activities, that aim to **improve the cybersecurity levels of European information infrastructures**, as well as **participation in other international activities and related groups**[7], will also be continued.

It is noted that the element of confidentiality must be taken into account during all cooperation and exchange of information and experiences with international organisations and working groups, as described in section 3.3 regarding the formation of the working groups.

Action 15 - Phase A – The Republic of Cyprus will continue to build upon its constructive cooperation with the rest of the European Union member states, through its representation and active contributions to relevant working groups and fora. This cooperation will support the actions and activities on a Union level to improve the level of cybersecurity in the whole of Europe.

3.14 Development of a National Contingency Plan for Critical Information Infrastructures

The measures and actions that have been discussed in preceding sections will contribute, to a large extent, to the improvement of cybersecurity in the Republic of Cyprus, including both the public and private sectors. The implementation of all of the actions in an organised and effective way will help reach the target of a safer and more secure information society.

However, no technological system or set of measures and actions, regardless of how comprehensive they are, will be able to protect cyberspace **to an absolute degree**, especially the critical information infrastructures of any country. Bearing this in mind, it is essential to develop a National Contingency Plan for Critical Information Infrastructures. The target of this plan will be to guide and develop detailed

[7] E.g. IMPACT (International Multilateral Partnership Against Cyber Threats).

processes and measures that will be taken when a large scale crisis affects the operations of critical information infrastructures (as will be defined and identified in the relevant action described in section 3.6) in the Republic of Cyprus to a significant degree.

The creation and development of the National Contingency Plan will be performed in tandem with the identification of critical information infrastructures in the Republic of Cyprus, and will include the following activities:

- Designation of categories and hierarchies of critical infrastructures, based on their contribution to the operation of vital communications and information services,
- Designation of the level of protection required for each part of this infrastructure (e.g. redundancy, alternative routes, physical security, etc.) to minimise the effects of its potential damage or destruction,
- Development of early warning systems and processes to monitor critical infrastructures, potentially with the help of the CERTs,
- Creation of (or improvement of already existing) emergency communications networks which are independent from the main networks, and if possible, using alternative means of communication entirely (e.g. wired, mobile and satellite networks),
- Development of **comprehensive** communications and management processes, between critical information infrastructure operators, for the handling of a potential crisis and to achieve constructive collaboration between them,
- Organisation of regular national cyber exercises with realistic crisis scenarios (see section 3.10) to test and improve the processes developed above,
- Identification of all the critical information infrastructures that are connected to other countries, or which provide services that could affect information infrastructures in other countries,
- Identification of available resources in terms of equipment and infrastructure, where deemed useful or necessary, between the relevant departments and services, and the creation of synergies for covering each other's resources and services in emergencies.

ENISA has prepared a comprehensive document[8] which describes best practices for the development of National Contingency Plans for critical information infrastructures, and which will be taken into account for the development of the related plan for the Republic of Cyprus; it emphasises the importance of a comprehensive cybersecurity and protection of critical information infrastructures strategy as a basis. It is noted that these above provisions, where needed, will be leveraged for the contribution of Cyprus to the development of a wider European Contingency Plan for the protection of European critical information infrastructures, whose abnormal operation would have negative impact in more than one member state.

[8]ENISA Good Practice Guide on National Contingency Plans for Critical Information Infrastructure

Action 16 - Phase A – Development of a National Contingency Plan, which will contain detailed processes and measures that will be taken when a large scale crisis affects the operations of critical information infrastructures in the Republic of Cyprus to a significant degree, with the aim of maintaining their operation at an acceptable minimum level until full restoration.

3.15 Interdependencies

This Strategy places special emphasis on the interdependencies and interactions between the actions that are described, even though each one has its own specific and separate targets, for its successful completion. The strategic response to threats against network and information security must be approached in a holistic fashion and it needs to be understood that many of these actions have to be implemented in combination, with the target of maximal success of such a strategic response.

Interdependencies are also evident in other levels of this response. As can be seen in section 2.3, there are a number of competent authorities handling different aspects of security, each one with its own areas of responsibility. Despite the fact that duplication needs to be avoided, all interdependencies must be recognised and the cooperation between these authorities must be ensured so that the specialised knowledge and capabilities within each authority can be leveraged to maximum effect. These interdependencies are large in number, and so it is necessary to identify and study them, as well as incorporate them into any future actions or response plans that may be developed.

In addition to this, operators of critical information infrastructures must explore, as part of their activities to manage threats and risks and for the development of business continuity plans, the interdependencies that they have for the secure management of their infrastructures, at all levels. In other words, the following questions needs to be answered:

- On whom does the business depend in relation to security?
- Who depends on the business in relation to security?

It is noted that an initial depiction of the interdependencies between the actions described in this document can be found in Appendix II.

Action 17 - Phase A/B – Identification and study of the interdependencies that exist for the implementation of this Strategy. These interdependencies will initially be identified as existing in the relationships between the actions themselves, the relationships between the competent authorities of the State, and the relationships between the critical infrastructure operators with their suppliers, customers and staff. These interdependencies must be recognised and accepted by all relevant stakeholders.

4. NEXT STEPS

4.1 Immediate Actions – Phase A

It has been deemed necessary that a number of the actions, that have been identified and described in this document, need to start immediately, independently of the implementation of the remaining provisions of the strategic response. Taking into account the activities that are prioritised in section 3.2, and their associated actions described herein, the following activities must begin in 2012: the identification of critical information infrastructures (section 3.6), the development of a National Contingency Plan for these infrastructures (section 3.14), ensuring the full operation of Computer Emergency Response Teams for incidents related to network and information security (CSIRT/CERT) and the planning and participation of Cyprus in the pan-European exercise Cyber Europe 2012 (section 3.10).

Specifically, the actions to be performed within Phase A are as follows:

- Action 1 – Collaboration Framework
- Action 2 - Organisational Structure
- Action 3 (partial implementation) – Creating of Working Groups
- Action 5 (partial implementation) – Survey of the Private Sector
- Action 7 - Identification of Critical Information Infrastructures
- Action 10 – Ensuring the Full Operation of the CERTs
- Action 12 – National and International Exercises
- Action 15 – International Cooperation
- Action 16 - Development of a National Contingency Plan for Critical Information Infrastructures
- Action 17 – (partial implementation) Modelling and Analysis of Interdependencies.

This document provides synopses of the most important actions that have been identified for a coherent strategic response, so that cyberspace (and more generally the networks and information that are used on a daily basis) is secured, across the whole of Cypriot society. However, for correct implementation, each action needs to be analysed and expanded in detail, so that all associated activities can be identified. A detailed analysis of each of the actions in the strategic response will follow, as well as the identification of the resources and processes that will be needed for the implementation.

4.2 Cost of Implementation

In the context of detailed assessment and analysis of the individual actions, to the point to which it is feasible, the cost of implementing each action, as well as the time periods where specific budget items will be required, will be identified. This costing process will be undertaken in cooperation with the competent authorities, and always bearing in mind the importance of each action and range of its application, so that the costing can be as realistic as possible.

In parallel with this costing, the actions described in this document will be prioritised (independently of their estimated cost), as to their importance and criticality in relation to the results that they are expected to provide towards a safer electronic environment in the Republic of Cyprus. It is noted that this activity will be undertaken independently of the costing process for the actions that is described above.

4.3 Planning of Actions 2012 - 2015

The activities mentioned in sections 4.1 and 4.2 are important so that the correct planning of the strategic response actions can move forward, based on the resources that the State will make available for the implementation of this Strategy. This planning will be undertaken based on the results of the detailed assessment, costing and prioritisation of the actions, so that the implementation of the Strategic Response as a whole can be achieved in the best and most effective way possible, given available resources. The result of this process will be a detailed timeline which will allow the monitoring of the implementation status of all of the current Strategy's actions.

4.4 Results Assessment and Strategy Review

To achieve an effective strategic response, its implementation progress must be regularly and strictly reviewed. Towards this end, the results of the implementation of the measures and provisions included in the strategy actions will be analysed quantitatively and qualitatively accordingly. A proper cybersecurity strategy cannot be considered to be a 'final plan'; on the contrary, its implementation must be observed and updated at regular intervals. This review process needs to take into consideration the assessment results, as well as new threats that appear (and will continue to appear) in cyberspace and any other new conditions that manifest in this area.

The detailed expansion of the strategy actions, as described in section 4.1, will include indicators and criteria for assessing the performance of each action, where feasible, and the results of this assessment will allow the proper review of the Strategy in the future, with substantial benefits to Cypriot society.

APPENDIX I - OVERVIEW OF STRATEGY ACTIONS

- **Phase A**
  - Phase A includes all of the actions that OCECPR is in a position to start in the immediate future with the resources that are currently available to it.
- **Phase B**
  - Phase B includes the actions that OCECPR will be in a position to coordinate once a new organisational structure has been developed, with the necessary resources to carry out the implementation of this Strategy in its entirety.

APPENDIX II - ACTION INTERDEPENDENCIES

The diagram below shows the indicative interdependencies between the Strategy actions. The significance of the formation of the working groups, for the correct implementation of the Strategy, is evident.