THE NATIONAL

CYBER SECURITY STRATEGY OF

THE REPUBLIC OF CROATIA

- Zagreb, 7 October 2015 (Official Gazette No 108/2015) -

TABLE OF CONTENTS

1. INTRODUCTION

Nowhere has technological development been more dynamic and comprehensive than in the area of communication and information technology. The focus has always been on the rapid development and introduction of new services and products, while the security-related aspects usually had little influence on the broad acceptance of new technologies.

The life cycles of modern-day information systems, from the process of planning, introduction and usage to their withdrawal from use are very short, which often makes their systematic testing impossible and is most commonly applied as an exception, in expressly prescribed cases.

Users usually have minimal knowledge of the technology they are using, and the technology is applied in such a way that makes it very hard to estimate the security characteristics of the majority of commercial products regarding the protection of user data confidentiality and privacy. Due to that, users' attitude towards the communication and information technology is based almost exclusively on blind confidence.

Modern societies are deeply imbued with communication and information technology. People are nowadays connected using various technologies for the transmission of text, image and sound, including the increasing Internet of Things (IoT) trend.

While a deviation in the normal functioning of a certain kind of communication and information system could go unnoticed, improper operation of some other systems could have harsh consequences for the functioning of the State; it can cause loss of life, damage to health, great material damage, pollution of the environment and the disturbance of other functionalities essential for the proper functioning of the society as a whole.

From the beginning of the development of communication and information technologies until the present day, deviations in their proper functioning have occurred due to different reasons, from human error or malicious action to technological error or organizational omission.

The creation of the Internet and connecting a number of communication and information systems of the public, academic and economic sectors, as well as citizens, created the contemporary cyberspace composed not only of this interconnected infrastructure, but also of the ever growing amounts of available information, and users communicating increasingly among themselves using a growing number of different services - some completely new, some traditional, but in a new, virtual form.

Deviations in the proper operation of these interconnected systems or their parts are no longer merely technical difficulties; they pose a danger with a global security impact. Modern societies counter them with a range of activities and measures collectively called "cyber security".

The term "cyber" entered the Croatian legal system upon the ratification of the Budapest Convention on Cybercrime[1] back in 2002. Following from that, the term "cyber" is most

[1] Act on the Ratification of the Convention on Cybercrime (Official Gazette No 09/02) and Act on the Ratification of the Additional Protocol to the Convention on Cybercrime, concerning criminalisation of acts of a racist and xenophobic nature committed through computer systems (Official Gazette No 04/08).

commonly used as an adjective describing something that includes, uses, or is related to computers and especially the Internet.

The original term "cybernetics" ("kibernetika" in Croatian) was formed in the mid-twentieth century and it denotes a science of automatic control systems and control processes in biological, technical, economic and other systems in general. The adjectival form "cybernetic" ("kibernetički" in Croatian) is used nowadays in the Croatian language in a similar way, with the same, previously introduced meaning as the prefix "cyber-" has in the English language. The term "cybernetics" is nowadays rarely used in the Croatian language with its original meaning, like the term "cybernetics" in the English language. The term predominantly used in technical sciences dealing with systems control is "automatic control". The term much more common, in the broader sense of meaning of the concept of cybernetics, referring to control processes in different systems, is "systems theory", introduced in the second half of the past century.

Recognising the importance of security within cyberspace as a common responsibility of all the society's segments prompted the making of this Strategy. Its purpose is achieving a systematic and coordinated implementation of the activities necessary for improving Croatia's capabilities in the area of cyber security, with a view to building a safe society in cyberspace. The goal is also to take advantage of the full market potential of the information society as a whole, and especially cyber security products and services.

Since this is the first comprehensive Croatian Strategy in the area of cyber security, the Strategy's primary objective is to recognise organisational problems in its implementation and broaden the understanding of the importance of this issue in the society.

In order to establish new functionalities, improve the efficiency of the relevant actors' work, use more efficiently the existing resources and better plan the requirements and establishment of new resources, it is necessary to encourage coordination and cooperation of all the state authorities, legal entities with public authority and other society sectors.

Therefore, the Strategy's fundamental role is to connect and bring mutual understanding of this complex issue in various sectors of the society and among various bodies and legal entities as the stakeholders of this Strategy with different competences, responsibilities, tasks, needs, expectations and interests. This is particularly important for ensuring the required level of understanding of the complex operational and technical issues of cyber security, which is necessary for the central public authorities and decision makers in all the sectors of the society, as it is for the security of the citizens, prosperity of the entire society, and thus for the end goal of this Strategy: implementing the law and respecting all the fundamental human rights in the new, virtual dimension of the society.

In order to cover the very broad and complex area of this Strategy and harmonise the joint efforts of the numerous stakeholders that participated in the making of this Strategy, the method applied for developing its contents included defining the basic principles of approach to the area of cyber security, defining the objectives of the Strategy, and the scope of application of the Strategy in relation to the entire society.

Following from the above, Croatia's priority areas of cyber security were determined and they were analysed primarily in relation to the general goals of the Strategy. Special objectives

were defined in the same way for each of the cyber security areas determined in the Strategy. Implementation measures for those objectives will be elaborated in more detail in the action plan for the implementation of the Strategy. In this way it was possible to also include the particularities of each individual area related to the society sectors defined by the Strategy and forms of mutual cooperation and coordination of various cyber security stakeholders.

The interrelations of cyber security areas were defined in order to also cover those cyber security segments which, according to estimates, are common for most or all of the previously determined cyber security areas. The interrelations of cyber security areas are very important for improving and achieving more efficiently the objectives and measures in cyber security areas. Special objectives are therefore also defined in the Strategy for the interrelations of cyber security areas. Those objectives are considered to have key importance in improving the level of security in cyberspace. Special attention is again focussed on the sectors of the society defined in the Strategy, as well as forms of cooperation and coordination of the efforts of cyber security stakeholders.

2. PRINCIPLES

Comprehensive nature of the approach to cyber security by covering cyberspace, infrastructure and users under the Croatian jurisdiction (citizenship, registration, domain, address);

Integration of activities and measures arising from different cyber security areas and their interconnection and supplementation in order to create a safer cyberspace;

Proactive approach through constant adjustment of activities and measures, and adequate periodic adaptation of the strategic framework they stem from;

Strengthening resilience, reliability and adjustability by applying universal criteria of confidentiality, integrity and availability of certain groups of information and recognised social values, in addition to complying with the appropriate obligations related to the protection of privacy, as well as confidentiality, integrity and availability for certain groups of information, including the implementation of appropriate certification and accreditation of different kinds of devices and systems, and also business processes in which such information is used;

Application of basic principles as basis of the organisation of modern society in the area of cyberspace as the society's virtual dimension:

1. **Application of law** to protect human rights and liberties, especially privacy, ownership and all other essential characteristics of an organized contemporary society;
2. **Developing a harmonised legal framework** through continued improvement of all the segments of regulatory mechanisms of state and sector levels, and through harmonised initiatives of all the sectors of the society, that is, bodies and legal entities that are stakeholders in this Strategy;
3. **Application of the principle of subsidiarity** through a systematically elaborated transfer of power to make decisions and report on cyber security issues to the appropriate authority whose competences are closest to the matter being resolved in areas important for cyber security, from organization through coordination and cooperation to the technical issues of responding to computer threats to certain communication and information infrastructure;
4. **Application of the principle of proportionality** to make the level of protection increase and related costs in each area proportional to the related risks and abilities in limiting the threats causing them.

3. GENERAL GOALS OF THE STRATEGY

1. **Systematic approach in the application and enhancement of the national legal framework** to take into account the new, cyber dimension of the society, keeping in mind the harmonisation with international obligations and global cyber security trends;
2. **Pursuing activities and measures to increase the security, resilience and reliability of cyberspace**, which need to be applied in order to ensure the availability, integrity and confidentiality of the respective groups of information used in cyberspace, both by the providers of various electronic and infrastructure services and by the users, namely all legal entities and individuals whose information systems are connected to cyberspace;
3. **Establishing a more efficient mechanism of information sharing** necessary for ensuring a higher level of general security in cyberspace, whereby each stakeholder is required, especially concerning certain groups of information, to ensure the implementation of adequate and harmonised standards of data protection;
4. **Raising security awareness** of all cyberspace users with an approach that distinguishes between the particularities of the public and economic sectors, legal entities and individuals, and which includes the introduction of the necessary educational elements into regular and extracurricular school activities, along with organising and implementing various activities aimed at making the broader public aware of certain current issues in this domain;
5. **Stimulating the development of harmonised education programmes** in schools and higher education institutions, through targeted and specialist courses, by connecting the academic, public and economic sectors;
6. **Stimulating the development of e-services** through building user confidence in e-services by defining the appropriate minimum security requirements;
7. **Stimulating research and development** in order to activate the potential and encourage harmonised efforts of the academic, economic and public sectors;
8. **Systematic approach to international cooperation** which makes possible an efficient transfer of knowledge and coordinated information sharing amongst the different competent national authorities, institutions and sectors of the society, with a view to recognising and creating capabilities for successful participation in business activities in a global environment.

4. SECTORS OF THE SOCIETY AND FORMS OF COOPERATION OF CYBER SECURITY STAKEHOLDERS

Defining the sectors of the society and their meaning for the purposes of this Strategy, as well as forms of cooperation of the cyber security stakeholders, also provided the definition of the scope of this Strategy.

For the purposes of the Strategy, sectors of the society and their definitions are:

1. **Public sector** with various competent authorities which are the stakeholders of the Strategy, other state authorities, bodies of local and regional self-government units, legal entities with public authorities and institutions representing in various ways the users of cyberspace and entities obliged to apply the measures arising from the Strategy;
2. **Academic sector** in close cooperation with the state authorities which are the stakeholders of the Strategy, and other education institutions from the public and economic sectors representing in various ways the users of cyberspace and entities obliged to apply the measures arising from the Strategy;
3. **Economic sector** in close cooperation with the competent state and regulatory bodies which are the stakeholders of the Strategy, especially legal entities subject to special regulations concerning critical infrastructures and defence, as well as all other legal entities and business entities representing in various ways the users of cyberspace and entities obliged to apply the measures arising from the Strategy, with all the particularities of those legal and business entities, with regard to their scope of work, number of employees and markets they cover;
4. **Citizens** in general, representing the users of communication and information technologies and services. The state of security in cyberspace reflects on the citizens in various ways. It also refers to the citizens who do not use cyberspace actively, but their data is in cyberspace.

Forms of cooperation of cyber security stakeholders envisaged by the Strategy are:

1. **Coordination within the public sector**;
2. **National cooperation of the public, academic and economic sectors**;
3. **Consultation with the interested public and informing the citizens;**
4. **International cooperation of cyber security stakeholders.**

All these forms of cooperation are carried out in a systematic and coordinated manner, in accordance with competences, capabilities and objectives, and according to the functionally elaborated cyber security areas defined in the Strategy.

5. CYBER SECURITY AREAS

Cyber security areas are defined in accordance with the evaluation of Croatia's priority needs at the time of drafting the Strategy and they cover the security measures in the area of communication and information infrastructure and services, where we have public electronic communications, e-Government and electronic financial services as infrastructure of primary strategic interest for the entire society.

Protection of critical communication and information infrastructure is also a very important area of cyber security. It may be present in each of the three infrastructure areas mentioned above, but has significantly different characteristics and it is necessary to determine the criteria for recognising those characteristics.

Cybercrime has been present in the society for a long time in different forms, but at today's level of development of the society's virtual dimension it poses a constant and growing threat to the development and economic prosperity of every modern state. That is why countering cybercrime is also considered a priority cyber security area and it is necessary to define the strategic goals to improve the efforts in countering this type of crime in the coming period.

The area of cyber defence represents the part of the defence strategy falling under the responsibility of the ministry in charge of defence issues. It is the subject of separate elaboration and action, which will be pursued using all the necessary elements arising from this Strategy. Cyberterrorism and other cyber aspects of national security are dealt with by a small number of the competent bodies within the security and intelligence system and require a separate approach, and that will also include the use of all the necessary elements arising from this Strategy.

Cyber security areas are analysed in relation to the general goals of the Strategy in order to identify the special objectives aimed at achieving improvements in each individual area and the measures necessary for achieving the goals of the Strategy. The special objectives, as well as the measures that will be further elaborated by the Action plan for the implementation of the Strategy, are determined with regard to the defined society sectors and the influence of the cyber security area on each individual sector, but also with regard to the forms of mutual cooperation and coordination of cyber security stakeholders. The principles defined by the Strategy are followed in the elaboration of the cyber security areas.

5.1 Electronic communication and information infrastructure and services

5.1.1 Public electronic communications (A)

Public electronic communications include the provision of an electronic communications network and/or the provision of an electronic communications service. Electronic communication and information infrastructure, performing of activities including electronic communication networks and services, spatial planning, building, maintenance, development and use of electronic communication networks, electronic communication infrastructure and

other related equipment, as well as managing and using the radio frequency spectrum, address space and numbering, as the naturally limited public goods, are of interest for the Republic of Croatia.

The legal, regulatory and technical provisions adopted at the EU level, related to data protection, privacy and legitimate interests of legal entities in the area of electronic communications, require continued harmonisation in order to make sure that there will be no impediments to promoting and developing new electronic communication networks and services among the EU Member States.

The basic objectives of the Republic of Croatia related to cyber security in the area of public electronic communications are:

Objective A.1 *Inspection of technical and organizational measures taken by operators to ensure the security of their networks and services, and directing the operators of public communication networks and/or services with the aim of ensuring a high level of security and availability of public communication networks and services.*

It is necessary to cover the various requirements imposed on the operators, from quality and availability of networks and services, through requirements regarding data protection, requirements for ensuring adequate attention in implementing security measures based on the appropriate international standards, requirements for implementing legal obligations of secret surveillance of electronic communication networks and services, to the necessity of developing and constantly improving security cooperation and information exchange with the bodies responsible for computer security incidents in the area of public electronic communications and criminal prosecution authorities.

Objective A.2 *Direct technical coordination between the national regulatory authority for the area of electronic communications and national and international authorities responsible for the area of information security.*

It is necessary to establish and continuously develop inter-sectoral collaboration of national regulatory authorities and authorities responsible for the area of information security and data protection policy, and establish coordination and exchange of experiences in cooperation and requirements arising from the international framework.

Objective A.3 *Encouraging the providers of public communication networks and/or services to use the national centre for Internet exchange in providing services to users in Croatia.*

The non-profit service Croatian Internet eXchange (CIX) provides mutual exchange of internet traffic among the users of different service operators using the shortest communication path within the national system of public electronic communications. This kind of Internet exchange represents a security requirement for operators providing services to state authorities, but it also calls for efficient and economic national-level connecting of all the other economic sector users and citizens of the Republic of Croatia.

5.1.2 E-Government (B)

E-Government is Croatia's strategic goal, ensuring a quick, transparent and secure service for all citizens via cyberspace. For this purpose it is necessary to establish a system of public registries and operate it on the basis of clearly defined rights, obligations and responsibilities of the competent public sector bodies. In order to ensure the necessary level of security for the information stored in such registries, a common base has to be used for secure exchange of information within the system of the government information infrastructure - a federated identification and authentication system (NIAS in Croatia, see Footnote 2). The Republic of Croatia will continue developing and improving its electronic communication with the citizens. It will also continue interconnecting the state bodies and bodies of the public sector in general. Special attention will be paid to:

1. Availability of information from public registries to all public sector bodies, citizens and other users in accordance with regulations on personal data protection, secrecy of information, information security and regulations on the right of access to public information;
2. Systematic development of the government information infrastructure, including spatial planning, building, maintenance, development and use of electronic communication networks and infrastructure for the needs of the public sector;
3. Systematic protection and security of government information infrastructure in accordance with information systems security regulations;
4. Croatian Government's central management of the development of government information infrastructure, based on the agreed requirements and priorities;
5. Harmonising informatization plans and projects with the standards and other determinants regarding the building of information infrastructure in Croatia and the European Union;
6. Interoperability, scalability and information re-use;
7. Rationalisation of expenditure on building and protection of information infrastructure at the level of all public sector bodies.

Objective B.1 *Encouraging the interconnecting of information systems of public sector bodies and their connecting to the public Internet using government information infrastructure.*

Public sector bodies that are not covered by the law regulating the area of government information infrastructure will, in cooperation with the state bodies competent for the development and security of government information infrastructure, conduct an analysis of the needs and capabilities of connecting to the government information infrastructure and, based on its results, plan the connection to the government information infrastructure or additional protection measures.

Objective B.2 *Raising the security level of public sector information systems.*

The current state of implementation of information systems security measures in public sector bodies will be analysed and the dynamics will be defined for the application of the NIAS system and the appropriate standards (ISO 27001, etc.). Organizational and technical

standards for connecting to government information infrastructure; conditions and activities necessary to launch, implement, develop and monitor projects related to government information infrastructure; management, development and other elements necessary for the functioning of government information infrastructure will be continuously evaluated through the coordination of the competent bodies, including security authorities.

Objective B.3 *Establishing criteria for use of certain authentication levels among e-Government service providers and credentials providers.*

The standard single-factor authentication, i.e. level 2 credentials according to the document "The criteria for determining the level of authentication quality assurance for NIAS"[2], is not at a satisfactory security level for access to sensitive information. A satisfactory solution, in terms of reducing security risks, which is also acceptable for use in the framework of e-Government services, is using the credentials of higher (level 3) or highest (level 4) security levels. The competent authorities will conduct an analysis and work in a coordinated manner in order to establish the criteria for use of certain authentication levels among the e-Government service providers and credentials providers. The analysis will also include an assessment of possibilities of using the e-Citizens ID card for the purposes of e-Government and other public and financial services. It will also cover other aspects related to national possibilities to establish the appropriate accreditation and certification capabilities in the area of qualified electronic signatures, in accordance with the EU requirements.

5.1.3 Electronic financial services (C)

Information technology and its benefits are also widely used in the area of providing financial services. Achieving satisfactory levels of security is the goal of every modern state, and the basic goals of the Republic of Croatia related to cyber security in the field of electronic financial services are:

Objective C.1 *Undertaking activities and measures for increasing the security, resilience and reliability of cyberspace, with the aim of stimulating the development of electronic financial services.*

Continually stimulate the providers of electronic financial services to introduce new mechanisms of protection against malicious activities and improve the existing ones, in accordance with current threats and risk assessments. In doing so, special attention has to be given to the identification and authentication of the users of electronic financial services, authorization of financial transactions and timely detection and limitation of the impact of unauthorized activity.

[2] https://www.gov.hr/UserDocsImages//e-Gradjani_dok//NIAS%20-%20Kriteriji%20za%20odredjivanje%20razine%20osiguranja%20kvalitete%20autentifikacije%20u%20sustavu%20NIAS%20(Ver.%201.2).pdf (in Croatian)

Objective C.2 *Enhance information sharing about computer security incidents among the providers of electronic financial services, regulatory and supervisory bodies and other relevant authorities.*

Creating the conditions for the implementation of efficient information sharing, which will also improve the process of treating computer security incidents, prevent the occurrence of such incidents in the future or ensure that their impact is limited. Particular attention has to be paid to the protection of personal data and other information covered by legal restrictions related to information use and information sharing, building trust among the parties involved, and establishing protocols and mechanisms that will ensure efficient and secure collection of information and information sharing. Computer security incident related information sharing includes the providers of electronic financial services, regulatory and supervisory bodies, bodies competent for computer security incidents in the area of public electronic communications, and criminal prosecution authorities.

5.2 Critical communication and information infrastructure and cyber crisis management (D)

The enactment of the Act on Critical Infrastructures[3] and subordinate legislation created the legislative preconditions for successful risk management in the critical communication and information infrastructure, within the designated critical infrastructure sectors, in order to:

1. Increase the resilience/reduce the vulnerability of communication and information systems;
2. Mitigate the consequences of negative events (natural disasters and technical-technological accidents) and possible attacks (intentional and unintentional);
3. Enable quick and efficient recovery and resumption of operation.

Pursuant to the Decision of the Croatian Government[4], the sector of communication and information technology has been designated as one of the sectors from which the central state administration bodies identify critical national infrastructures by applying the appropriate method. Its subsectors have been designated as follows: electronic communications, data transmission, information systems and provision of audio and audio-visual media services. These subsectors are further divided into the following sections: electronic communication networks, infrastructure and the related equipment, information infrastructure and terrestrial radio broadcasting systems.

Continuation of activities in the area of critical communication and information infrastructure protection is a strategic interest, for the purpose of making all the necessary conditions for its functioning and continued operation.

[3] Published in the Official Gazette, No 56/13.

[4] Decision on designation of sectors from which central state administration bodies identify critical national infrastructures and critical infrastructures sector sequence list (Official Gazette 108/13).

Communication and information systems that run the critical infrastructure or are essential for its functioning represent critical communication and information infrastructure, regardless of which critical infrastructure sector they belong to.

It is therefore necessary that the identification of critical communication and information infrastructure and prescription of mandatory technical and organizational measures, including procedures of reporting about computer security incidents, be carried out in a coordinated manner by central state bodies responsible for certain critical infrastructure sectors, critical infrastructure owners/operators and competent technical and security-related state authorities.

In addition, establishing a cyber crisis management system that will ensure a timely and efficient reaction/response to a threat and the recovery of infrastructure or service is of particular interest to the Republic of Croatia in terms of security.

The system of cyber crisis management in Croatia needs to be established in accordance with the following requirements:

1. Harmonisation with the national crisis management solutions,
2. Inclusion of the protection of critical national communication and information infrastructure,
3. Harmonisation with international cyber crisis management systems of the EU and NATO,
4. Harmonisation with national competences of the bodies legally responsible for the coordination of the prevention of and the response to computer threats to the security of information systems.

In that sense, it is necessary to:

Objective D.1 *Determine criteria for identifying critical communication and information infrastructure.*

The criteria for identifying critical communication and information infrastructure must follow and further elaborate the methodology of approach envisaged by the Act on Critical Infrastructures. Critical communication and information infrastructure is determined in the framework of the sectors designated by the aforementioned Decision of the Croatian Government on designation of sectors from which central state administration bodies identify critical national infrastructures and critical infrastructures sector sequence list. The criteria defined for designating critical communication and information infrastructure must arise from the methodology applied by the Act on Critical Infrastructures. If the situation analysis proves it necessary, they can be further elaborated and prescribed by the appropriate subordinate legislation.

Objective D.2 *Determine binding security measures to be applied by owners/operators of designated critical communication and information infrastructure.*

It is necessary to determine a set of security measures to be applied systematically by all the designated owners/operators of critical communication and information infrastructure, as well as the necessary relation to the general information security regulations, in segments such as

personnel security clearance requirements or the need to determine a certain type of information as classified.

Objective D.3 *Strengthen prevention and protection through risk management.*

The priority is to ensure the implementation of the provisions of the Act on Critical Infrastructures in segments concerning the sector risk analysis of critical communication and information infrastructure, sector plans for ensuring the work of critical communication and information infrastructure, and security plans of owners/operators of critical communication and information infrastructure.

The sector risk analysis includes:

1. Identification of critical functions (procedures, information, networks, etc.);
2. Identification of threats;
3. Assessment of threats, vulnerabilities and impact;
4. Analysis and prioritisation of risks;
5. Determining acceptable risk and risk treatment.

Sector plans for ensuring the work of critical infrastructure and security plans of owners/operators of this critical infrastructure contain measures and activities for preparedness, prevention, protection, response and recovery in case of computer security incidents with adverse impact on the functioning of the critical infrastructure sector, namely production and delivery of goods and services and other functions of critical infrastructure owners/operators, the operation or functioning of which is based on critical communication and information infrastructure. Special attention has to be paid to the professional training of the individuals who will be involved in the procedure of designating critical communication and information infrastructure.

Objective D.4 *Strengthen public-private partnership and technical coordination in the treatment of computer security incidents.*

Within the sectors of critical infrastructure designated by the aforementioned Decision of the Croatian Government on designation of sectors from which central state administration bodies identify critical national infrastructures and critical infrastructures sector sequence list, it is necessary to encourage public-private partnership through central bodies of state government competent for certain sectors, in order to ensure unhindered functioning of the business entities representing the owners/operators of critical infrastructure. It is necessary to determine the appropriate procedures of oversight, coordination, and information sharing concerning the necessary security information. Information sharing is conducted among the competent sectoral entities and owners/operators of critical infrastructures, with bodies in charge of computer security incidents in areas of public electronic communication and information infrastructure and services, and with the criminal prosecution authorities. Technical coordination in the treatment of computer security incidents is undertaken through the cooperation of the bodies with developed capabilities in responding to such incidents.

Objective D.5 *Develop capacities for efficient response to a threat that may result in cyber crisis.*

It is necessary to build a national system of cyber crisis management in Croatia as part of the national crisis management system, where the responsibilities of the relevant participants will be uniformly defined on the basis of the authorities' existing competences and additional defining of the authorities' roles in cases that constitute crises.

The national cyber crisis management system has to ensure:

- Systematic monitoring of the state of security of the national cyberspace for the purpose of detecting threats that may result in cyber crisis,
- Periodic reporting on the state of cyber security,
- Efficient planning of actions during cyber crisis,
- Harmonised and coordinated action of state authorities during cyber crisis.

To that end, it is necessary to thoroughly analyse the current situation, especially in relation to the legal framework and any improvements it may require in the context of possible introduction of new competences necessary in dealing with this issue. Based on the results of the analysis, the definition of the concept of cyber crisis in the framework of a broader concept of the national level crisis management will be proposed, along with the criteria for identifying a cyber crisis.

5.3 Cybercrime (E)

Computer crime, or cybercrime, is crime that involves computer systems, programmes and data, committed in cyberspace by using communication and information technologies and poses a threat to achieving a safer information society.

The establishment of effective prevention measures, but also the criminal law response to this type of crime, are the key elements for achieving the appropriate level of protected, unobstructed operation and security of computer systems.

High-quality and successful countering of this form of crime requires:

Objective E.1 *Continued enhancement of national legislation, taking into account international obligations.*

As rapid technological growth brings along new modalities of committing criminal offences using computer systems and networks, followed also by the development of legislation in this domain at the international level, it is necessary to constantly monitor, analyse and, if needed, amend the national legislation in accordance with the emerging changes.

Objective E.2 *Improve and stimulate international cooperation for efficient information sharing.*

The globalisation of cybercrime as a phenomenon in which the perpetrators know no physical state borders, legislation differences in the states in which they act and ignore language

barriers, requires close cooperation of the EU and NATO Member States and international cooperation with third countries, for the purpose of timely identification of every new form or threat, as well as their source, and in order for the response to a certain threat to follow as quickly as possible. It is therefore necessary to use the available possibilities of the existing cooperation models through contact points and the possibilities of swift information sharing through the channels of Europol, Eurojust and other international organisations.

Objective E.3 *Good inter-institutional cooperation for efficient information exchange at national level, especially in case of computer security incident.*

A computer security incident requires quick and adequate treatment. It is necessary to establish high quality coordination of all the bodies that can contribute in a particular case. The existence of permanent "contact points" would contribute to direct and effective communication and thus also to the prevention and more efficient treatment of the incident.

Objective E.4 *Strengthening human resources, adequate development of relevant state bodies' competences and technical capabilities for discovering, conducting criminal investigation and prosecuting criminal cases in cybercrime domain, along with securing the necessary funding.*

The development of electronic communication infrastructure and introduction of new innovative services is accompanied by the emergence of new, increasingly sophisticated ways of committing criminal offences in cybercrime domain. These processes require continued strengthening of human resources, appropriate upgrading of forensic tools and systems, and systems for secret surveillance of electronic communication networks and services.

Objective E.5 *Encouragement and constant development of cooperation with economic sector.*

Encouragement and constant development of cooperation with the economic sector (especially with the national regulatory authorities and legal entities in the public electronic communications sector and the sector of electronic financial services), as well as information sharing about all the new computer security incidents that have been registered, to enable the economic sector to recognise a potential incident that could constitute a criminal offence and update its own security system in a timely manner, and to enable the state administration bodies to promptly react to a possible criminal offence. Additionally, good cooperation with the economic sector should be used to stimulate communication aimed at educating the end users of certain services, thus directly contributing to the prevention of a particular cybercrime occurrence.

6. INTERRELATIONS OF THE AREAS OF CYBER SECURITY

The interrelations of cyber security areas are defined in accordance with the assessment of Croatia's needs at the time of drafting the Strategy and they cover cyber security segments estimated to be common to all or most of the previously selected cyber security areas. The selected interrelations of cyber security areas are:

1. Protection of information;
2. Technical coordination in the treatment of computer security incidents;
3. International cooperation, and
4. Education, research, development and raising security awareness in cyberspace.

The interrelations of cyber security areas are essential for the improvement and more efficient achievement of the goals and measures in cyber security areas. The Strategy therefore also defines special objectives, regarding the interrelations, which are considered crucial for enhancing the level of security in cyberspace, with special reference to the defined society sectors and the influence of each interrelation of cyber security areas on certain sectors of the society and forms of cooperation and mutual coordination in the work of cyber security stakeholders. The elaboration of interrelations of cyber security areas is done according to the principles defined by the Strategy.

6.1 Protection of information (F)

In the life cycle of a piece of information, as soon as it is generated, it is necessary to determine whether it belongs to a certain group of protected information and apply the appropriate set of measures to protect such information. It is the responsibility of every protected information owner and data controller, but also every protected information processor and every authorised user of protected information, not only to take care of the confidentiality and privacy of the information they use in their work, but also to be accountable for the integrity and availability of the information that is released publicly in cyberspace (web sites, social networks, etc.).

In order to direct the handling of protected information in an appropriate manner, especially on the part of the entities responsible for protected information, the following groups of protected information were identified in drafting this Strategy as the most important special groups of protected information which require the implementation of adequate protection policy: classified information, unclassified[5] information, personal data and trade secret.

[5] Group of information appropriately marked, used only for official purposes in the government sector, which does not have the characteristic of being secret.

In cyber security areas identified by this Strategy there is a great need for information sharing concerning the information that in most cases represents one of the above mentioned special groups of protected information.

Each of these protected information groups is regulated by an appropriate package of acts and subordinate legislation, and the problems encountered so far in practice were in most cases related to the implementation policies of information protection, especially in legal entities, and to a broader lack of understanding and awareness in different society sectors of the need and necessity to develop a culture of handling certain groups of protected information.

The following is required in order to improve the state of security and provide all the prerequisites for unobstructed information sharing concerning such information among the different competent stakeholders involved in certain cyber security activities:

Objective F.1 *Improvement of national regulations in the area of trade secrets.*

It has been detected that there is room for improvement in the area of trade secrets at the national level, which should be consistent with the ongoing unification of this field started in 2013 by the EU among Member States. The current situation may lead to legal uncertainty and it is considered necessary to elaborate the criteria for designating and protecting trade secrets, with mandatory application of the duty of care principles by those responsible in using this group of protected information.

Objective F.2 *Encouraging continuous cooperation of authorities competent for special groups of protected information in national environment to achieve alignment in implementation of relevant regulations.*

It has been detected that interdepartmental and inter-sectoral coordination of the entire society is necessary for harmonising certain implementing elements of legal regulations. Emphasis is placed on the need and importance of exchange of experiences among the national and international authorities competent for certain groups of protected information in the national environment, as well as following all the current amendments to the rules regulating access to information, especially in the EU and NATO environment, and in the scope of the needs and obligations of Croatia as a member of the EU and NATO. Measures from the Action plan for the implementation of the Strategy have to focus the attention towards the institutions, namely all the entities responsible for protected information. The role of the entities responsible for protected information is to ensure a uniform approach to the implementation of the relevant regulations on the part of all the protected information processors. This also applies to the authorised users of such information in the framework of the appropriate internal information security policies implemented by those processors and users.

Objective F.3 *Determining criteria for identifying national electronic registries, which are critical information resources, and entities responsible for their protection.*

Inadequate policies of protecting information in national electronic registries are one of the important problems that have been detected. The problem lies in the cumulation of a large

amount of information from a certain group (e.g. data gathered for all citizens at the national level), which makes the vulnerability of such information resources critical for other interconnected information resources, too. It is necessary to analyse this area carefully and determine the criteria for defining national electronic registries which represent critical information resources, as well as the additional requirements for the protection of such critical information resources. This has to be conducted following the possibility of applying regulations on critical national infrastructures on the one hand and, on the other hand, possibly relating to the criteria for determining as classified the registries of information which, when put together in electronic form, become critical at the national level and in the sense described.

Objective F.4 *Improving the way protected information is handled by entities responsible for protected information, protected information processors and authorised users of protected information.*

Despite the satisfactory regulations, harmonised with international requirements of the EU and NATO, there is room for practical implementation improvements in the use and information sharing of both classified information and personal data, especially in relation to legal entities and the handling of electronic information, regardless of whether the legal entities appear as protected information processors or users. Special attention must be paid to the specificity of cyberspace and services based on computer infrastructure, software platforms or cloud development applications. It is necessary to develop adjusted contract supplement templates (appendices, annexes, clauses). These templates would be appropriately unified and prepared for various forms of practical application, thereby indicating to the entities obliged to apply legal regulations the details of implementation of all the obligations highly important for information protection. This would refer especially to contracts the implementation or conclusion of which requires access to and use of protected information. The particularities of cyberspace and e-services would also be covered, that is, the conditions of using infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). These issues are viewed in the context of certain groups of protected information and accompanying regulatory requirements, and with regard to the particularities of cyberspace and cloud computing services. The mentioned issues include: problems related to information that is not physically controlled by the owner in the course of transmission, processing or storing; problems related to different legal responsibilities of service providers within various legal frameworks (national, EU, third countries); related issues of the relevant national framework for identification, authentication and authorisation (IAA) of the users of certain electronic services in public and economic sectors.

Objective F.5 *Unification of approach in using the set of standards ISO/IEC 27000*[6]*.*

The set of standards ISO/IEC 27000 is used in several sectors of the society for protecting different groups of information (e.g. protection of personal data, protection of unclassified

[6] Set of international standards for the area of information security management, accepted as the Croatian standard "HRN ISO/IEC 27000".

information, guidelines of the Croatian central bank for credit institutions, rules of the national telecommunications regulatory authority for public electronic service providers). The competent sectoral authorities and the competent authorities for the defined groups of protected information should analyse the possibility of unifying the approach and adopting the positive experiences and best practices in the application of the same set of standards in a different application context, but with very similar application goals. This will provide more cost-effective solutions for all the entities obliged to implement regulations and, at the same time, ensure a better understanding of the best security practice and provide national-level solutions which will be much more efficient in terms of security.

6.2 Technical coordination in the treatment of computer security incidents (G)

Technical coordination is one of the primary functions to be applied in the treatment of computer security incidents which resulted in the disruption of availability, confidentiality or integrity of information, in order to return to the pre-incident state. Considering the technical sophistication of modern-day attacks, a high level of technical capability of the CERTs[7] personnel is crucial, as they are the bodies in charge of preventing and responding to computer security incidents. Further enhancement of inter-sectoral organisation and information sharing regarding computer security incidents represent the necessary conditions for efficient technical coordination, keeping in mind the protection of sensitive information (statistics, anonymization) for the purposes of incident treatment or regular reporting, and in order to get a clearer picture of the state of security in cyberspace at the national level in Croatia. The mentioned national level includes the consolidation of statistical indicators of society sectors through the competent CERTs for the national and sectoral levels. The services and user base of each CERT have to be clearly defined, in accordance with the principle of subsidiarity in responding. This principle refers to the activities of one or more CERTs responsible for communication and information infrastructure in which the computer security incident occurred and in which it is being treated. Especially important are the prevention activities requiring a small investment but offering the possibility of achieving significant effects and preventing major damage.

Technical coordination plays an important role in the treatment and resolution of computer security incidents and the following is necessary for its improvement:

Objective G.1 *Continuous enhancement of existing systems for collecting, analysing and storing information about computer security incidents and making sure that other information essential for quick and efficient treatment of such incidents is up-to-date.*

Collecting, analysing and storing information about computer security incidents is very important for monitoring the trends and situation in national cyberspace. Information about

[7] In the context of the Strategy, the term CERT refers to every organisational unit (or subunit including individuals) responsible for coordination, prevention of and protection against computer threats.

computer security incidents is collected in the competent CERTs according to the principle of subsidiarity, and it is consolidated and monitored in central sectoral authorities. Bearing in mind the particularities of the different society sectors and selected cyber security areas, types of information about computer security incidents will be defined, as well as the ways of and prerequisites for exchanging such information among the central sectoral authorities. Central sectoral authorities will submit periodical reports to the National Cyber Security Council[8] about the trends, situation and important incidents in the recent period. Central sectoral authorities will submit appropriate reports to sectoral stakeholders on computer security incidents. Special attention will be paid to the improvement of the existing systems for collecting, analysing and storing incident-related information.

Objective G.2 *Regular implementation of measures for improving security by issuing warnings and recommendations.*

The centrally collected information about computer security incidents has to be analysed, exchanged and shared with the competent national regulatory authority and other relevant stakeholders. Based on the analyses of that information and information collected in other ways, bodies responsible for the security of public information systems and bodies responsible for the security of government information systems will apply measures for improving the security by defining warnings and recommendations.

Objective G.3 *Establishing constant information sharing regarding computer security incidents, as well as relevant information and expertise in solving specific cybercrime cases.*

Information that becomes known to criminal prosecution authorities and the security and intelligence system bodies in solving cybercrime cases significantly contributes to the overall picture of cyber security in Croatia but also to better prevention. It is therefore necessary that those bodies and the competent CERTs constantly exchange the appropriate information to the extent possible considering the competences and needs of certain stakeholders. Other than exchanging technical information, cooperation is necessary in the area of expertise, especially in solving more complex cybercrime cases.

6.3 International cooperation (H)

Cyberspace and the related technologies and knowledge have an increasing role in the overall development of the society, including the political, security, economic and social dimensions. It is quite clear how necessary it is to apply the same principles of security, rule of law and guarantees of established rights and freedoms to all individuals and legal entities in this field of human activity, too, in the same way they are applied out of cyberspace. Considering the fact that the international aspect is self-evident in the development, production and use of

[8] See chapter 7.

information and communication equipment, software, services or networks, the need is also clear for coordinated action, at both the national and international level.

National interest and all the necessary activities will be pursued according to the principles, values and obligations based on the Croatian Constitution, the Charter of the United Nations, international law, international humanitarian law and the relevant legal and strategic frameworks of Croatia and the EU, as well as other international obligations arising from the membership in the United Nations, NATO, Council of Europe, Organization for Security and Cooperation in Europe and other multilateral platforms and initiatives.

Croatia's priorities in the area of cyber security at the international level include:

Objective H.1 *Strengthening and broadening international cooperation in foreign and security policy areas with partner states, especially within EU and NATO, including mutual cooperation with third states.*

Organising international cooperation of different cyber security stakeholders, aimed at applying a systematic approach to international cooperation. Coordination of international cooperation should be organised in such a manner as to harmonise the participation of competent national bodies in appropriate international meetings with partner bodies with corresponding competences. International cooperation has to be accompanied by appropriate reports of the competent national authorities as the key stakeholders in international activities. Those reports should be exchanged and shared with the other appropriate cyber security stakeholders with thematically related competences.

Objective H.2 *Strengthening of international legal framework, with emphasis on promoting and improving the implementation of the Council of Europe's Convention on Cybercrime and accompanying protocols.*

It is necessary to form close connections among the different cyber security stakeholders, especially those with diplomatic and judicial competences, in order to ensure Croatia's effective participation in the development of international legal framework and adequate harmonisation and development of the national legal framework in this area.

Objective H.3 *Continuation and development of bilateral and multilateral cooperation under existing and future agreements with international associations.*

In order to meet Croatia's obligations and improve the national capability in implementing joint activities in the area of cyber security, it is necessary to provide an efficient and clear framework of cooperation between cyber security stakeholders in Croatia and certain international partners and associations, staying in line with the national competences of the bodies engaged in such international cooperation.

Objective H.4 *Promoting a concept of trust-building in cyber security.*

Participation in diplomatic activities in the framework of international organisations and other forums, to contribute to Croatia's efforts directed towards trust-building aimed at reducing the risk of conflicts caused by the use of information and communication technologies.

Objective H.5 *Participating in and organising international civilian and military exercises and other expert programmes.*

Participating in international exercises and expert meetings in the area of cyber security and organising them is necessary for ensuring efficient development and strengthening of the capabilities for a coordinated national and international response to cyber security threats, as well as harmonisation, testing and improvement of the achieved implementation level of cooperative defence of cyberspace. In organising and participating in such activities it is necessary to follow and coordinate them with regard to national competences of certain bodies as stakeholders of Croatia's cyber security.

Objective H.6 *Strengthening cooperation in the area of risk management for European critical infrastructures.*

The Croatian Act on Critical Infrastructures defines the concept of European critical infrastructures and prescribes their designation and protection. In accordance with the Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Member States are required to cooperate, establish information sharing, and exchange experiences and best practices to achieve the best and most efficient protection of the identified European critical infrastructures.

6.4 Education, research, development and raising security awareness in cyberspace (I)

For building a safe society and using the market potential of the information security and information society as a whole, it is necessary to apply a systematic approach to raising the level of the entire society's competences in the area of cyber security.

Appropriate educational activities have to be directed towards the following target groups:

- Formal education participants - it is necessary to ensure that primary and secondary school pupils and students attending professional and university studies acquire knowledge of the dangers they can encounter in the virtual environment; skills and competences to successfully ensure their own safe use of information and communication technologies at all levels of formal education, and awareness of the need to protect personal data;
- Various population segments - including all population segments in the process of learning about information security through the concept of lifelong learning and raise awareness of the need for protection;
- Data controllers, personal data recipients, data processors and all other persons coming into contact with critical national infrastructures and databases containing groups of protected information - ensure a higher level of education in the area of cyber security and raise awareness of the need to protect electronic information;

– Experts who will be dealing with information security - develop graduate, postgraduate and specialist study programmes in accordance with market needs.

In order to achieve the goals of the Strategy, the following actions are required in the area of education, research, development and awareness raising:

1. Connect all educational institutions in order to systemise programmes and curricula, and avoid unnecessary paralleling or implementation of teaching programmes in information security of questionable quality. It is necessary to connect institutions such as the State School for Public Administration, Police Academy and Judicial Academy with the universities, especially the units with established and high-quality programmes in the area of information security, personal data protection, cybercrime, etc.
2. Raise the level of knowledge about information security in all the segments of the society with campaigns including public media.
3. Considering the insufficient education of pupils in the area of cyber security, except for their school IT, implement content related to cyber security awareness raising in other school subjects as interdisciplinary content.
4. Call pupils' and parents' attention to the threats in the information society in homeroom classes, PTA meetings, thematic lectures and other extracurricular activities.
5. Include cyber security topics in professional development programmes for teachers.
6. Include segment-specific cyber security topics in training programmes for civil servants.
7. Bind electronic service providers to provide information on the consequences of security risks and protection mechanisms for a particular product or service. Bind service providers to incorporate security measures and provide information on security-related issues and security implications for those services or products in a manner understandable to the user.
8. Define strategic research sectors in the area of information security (from the point of view of defensive and offensive technologies, methods, algorithms, devices, software and hardware). Encourage research teams and research projects in the area of information security according to the guidelines in areas of strategic interest for the Republic of Croatia in terms of research and practical application. Strategically enable Croatia to have capacities for research, development, production, verification, assessment and expert evaluation in the area of information security. Improve communication between the academic, economic and public sectors and information sharing regarding information security.

Croatia's basic objectives related to education, research, development and awareness raising in the area of cyber security are:

Objective I.1 *Development of human resources in the area of communication and information technology security.*

It is necessary to systematically educate persons involved in the implementation of education programmes (teachers, lecturers, head teachers, associate experts and others) about cyber security. Cyber security elements must be included into formal education programmes and systematically applied, especially in the four major education groups, from pre-school through primary and secondary education to higher education. Youth should be encouraged to deal with information security in a lawful way. Graduate, doctoral and specialist study programmes in the area of cyber security must be stimulated. It is necessary to plan and implement specialised training for civil servants, technical staff and other personnel using in various manners communication and information technologies or working on their protection and the protection of their users.

Objective I.2 *Developing and raising security awareness in cyberspace.*

It is necessary to establish mechanisms enabling cyberspace users and service providers to be constantly aware of how to use it safely. Targeted educational campaigns have to be launched to reach the wider public. According to the instructions of the sectoral regulatory authorities, service providers will conduct additional activities for adequate protection of service providers and users.

Objective I.3 *Development of national capabilities, research and stimulation of economy.*

The development of national capabilities in various areas of information security has to be stimulated, both in the academic sector through research, and in the economic sector through the development of new products and services. Government bodies will apply a coordinated approach to stimulate public-private partnership, connecting of the academic, state and economic sectors, and presenting and promoting the solutions developed in Croatia on the global market.

7. IMPLEMENTATION OF THE STRATEGY

Action plan for the implementation of the Strategy, made for the purpose of implementing the Strategy, elaborates the defined strategic goals and determines the implementation measures necessary for achieving those goals, along with the competent authorities and the list of deadlines for their implementation.

Action plan for the implementation of the Strategy allows for systematic oversight of the implementation of the Strategy and serves as a control mechanism which will show whether a certain measure has been implemented in its entirety and has produced the desired result, or it should be redefined in accordance with the new requirements.

In order to determine in due time whether the Strategy is achieving the desired results, namely if the defined goals are being accomplished and the established measures implemented within the planned time frame, it is necessary to set up a system of continuous monitoring of the implementation of the Strategy and Action plan, thus also setting up a mechanism for coordinating all the competent government bodies in creating the appropriate policies and responses to threats in cyberspace.

For the purpose of reviewing and improving the implementation of the Strategy and Action plan for its implementation, the Government of the Republic of Croatia will establish the National Cyber Security Council[9] (hereinafter "the National Council"), which will:

- Systematically monitor and coordinate the implementation of the Strategy and discuss all issues relevant to cyber security,
- Propose measures to improve the implementation of the Strategy and Action plan for the implementation of the Strategy,
- Propose the organisation of national exercises in the area of cyber security,
- Issue recommendations, opinions, reports and guidelines related to the implementation of the Strategy and Action plan, and
- Propose amendments to the Strategy and Action plan or propose the adoption of a new Strategy and action plans, in accordance with the new requirements.

Based on the requirements described in the area of cyber crisis management, the National Council will:

- Address issues essential for cyber crisis management and propose measures for higher efficiency,
- Analyse the reports on the state of security submitted by the Operational and Technical Cyber Security Coordination Group,
- Issue periodic assessments of the state of security,

[9] Interdepartmental panel composed of the authorised representatives of the competent bodies with national or sectoral policy and coordination responsibilities.

- Define cyber crisis action plans,
- Issue programmes and action plans for the Operational and Technical Cyber Security Coordination Group and direct its work.

To ensure the support for the work of the National Council, the Government of the Republic of Croatia will establish the Operational and Technical Cyber Security Coordination Group[10], which will:

- Monitor the state of security in national cyberspace for the purpose of detecting threats that may result in cyber crisis,
- Issue reports on the state of cyber security,
- Propose cyber crisis action plans,
- Perform other duties according to the issued programmes and activity plans.

The representatives in the interdepartmental body, the Operational and Technical Cyber Security Coordination Group, mutually ensure access to operational information from their scope for the purpose of coordinated action during cyber crises.

The entities tasked with the measures from the Action plan for the implementation of the Strategy are responsible for monitoring and collecting information on the implementation and efficiency of the measures and are required to submit consolidated reports to the National Council once a year, no later than the end of the first quarter of the current year for the previous year or, if necessary, more frequently, namely at the request of the National Council.

The National Council will submit the reports on the implementation of the Action plan for the implementation of the Strategy to the Government of the Republic of Croatia no later than the end of the second quarter of the current year for the previous year.

The Strategy will be revised after three years of implementation, based on the reports of the entities tasked with the measures from the Action plan for the implementation of the Strategy. The National Council shall submit to the Government of the Republic of Croatia a consolidated report with the proposed amendments to the Strategy no later than the end of the year of revision.

[10] Interdepartmental panel composed of the authorised representatives of the competent bodies with operational and technical responsibilities.

APPENDIX: TERMS AND ACRONYMS

Terms

Authorised users of protected information - users of protected information whose authorisation, i.e. right of use, is based on legal or contractual basis, but who are not entities responsible for protected information or protected information processors.

Computer security incident - one or more computer security events that have disturbed or are disturbing the security of the information system.

Credentials - set of information used for introducing the user of electronic service, which serves as proof for electronic identity (e-ID) verification, in order to grant access to electronic services (e-services).

Critical communication and information infrastructure - communication and information systems whose disturbed functioning would significantly disturb the work of one or more identified critical national infrastructures.

Cyber (computer) crime - criminal offences against computer systems, software support and data; committed in cyberspace using information and communication technologies.

Cyber crisis - event or events in cyberspace which could cause or have already caused a significant disturbance in Croatia's social, political and economic life. Such a situation can eventually affect the security of people, democratic system, political stability, economy, environment and other national values, that is, national security and defence in general.

Cyber security - encompasses activities and measures for achieving the confidentiality, integrity and availability of information and systems in cyberspace.

Cyberspace - space in which communication among information systems takes place. In the context of the Strategy, it encompasses the Internet and all the systems connected to it.

Electronic communication and information infrastructure - includes computer and communication systems and software support used for data transmission, processing, storing.

Electronic communication and information services - commercial and non-commercial services provided using information and communication systems.

Electronic financial services - financial services provided directly to users by their authorised providers via electronic communication and information infrastructure (e.g. online and mobile banking, ATMs, EFTPOS systems).

Electronic financial service providers - subjects authorised by the competent authority to provide electronic financial services.

Entities responsible for protected information - protected information owners and information controllers.

Financial services - services in the area of banking, funds transfer, securities market, investment fund shares, insurance, leasing and factoring.

Government information infrastructure - consists of the common government base for secure information exchange and information exchange tools such as metaregistry, technical standards, classifications, public registries, NIAS, the e-Citizens system, and the government information infrastructure networks HITRONet and CARNet.

Identification and authentication system - system for establishing and verifying the identity of individuals, devices or services in information systems.

Information - different groups of electronic records which are of value to the users that handle them.

Information security - the state of confidentiality, integrity and availability of information, achieved by the application of appropriate security measures.

Internet - global network connecting various internet networks based on the TCP/IP protocol (such as CARNet or HITRONet in Croatia).

Protected information - information which, due to its content, has special importance to the values protected in a democratic society, for which reason it is recognised by the state as classified information, unclassified information, personal data or trade secret, and to which specific handling requirements apply in relation to information characteristics such as confidentiality, integrity, availability and privacy.

Protected information processing - every action or set of actions performed on protected information, such as collection, recording, organising, storing, adaption or alteration, withdrawal, consultation, usage, transmission, publishing, or making it otherwise available, alignment or combining, blocking, erasure or destruction, and performing logical, mathematical and other operations on such information.

Protected information processors - individuals or legal entities, state authorities or other bodies that process protected information on behalf of the entity responsible for protected information.

Security measures - general rules of information protection implemented at physical, technical or organisational level.

Sensitive information - groups of information used only for official purposes, or groups of information protected by appropriate regulations, but not having the characteristic of being secret (e.g. personal data or unclassified information, i.e. marked information for official use only).

Acronyms

CARNet	Croatian Academic and Research Network – academic network infrastructure.
CERT	(Computer Emergency Response Team) Common acronym for a group of experts responsible for treating security incidents in computer networks. In the context of the Strategy, the acronym CERT is used for any organisational unit, sub-unit or individual responsible for coordination, prevention of and protection from computer threats to information systems security. Other than CERT, the acronym CSIRT (Computer Security Incident Response Team) also exists in international practice.
Croatian Internet eXchange (CIX)	Croatian national centre for Internet exchange hosted at the University Computing Centre (Srce), open to all internet service providers in Croatia (for commercial and non-commercial or private networks).
EFU	Electronic financial services.
e-Citizens	The e-Citizens system is part of the government information system. It consists of the central state portal, national identification and authentication system and users' personal mailbox system.
EU	European Union.
e-service	Electronic service.
EUROJUST	The European Union's Judicial Cooperation Unit.
EUROPOL	The European Police Office.
EFTPOS system	Electronic Fund Transfer Point Of Sale - point of sale terminal for non-cash payment in which transactions are processed electronically.
HITRONet	Computer communication network of state administration bodies.
ISO/IEC 27000	Set of international standards for the area of information security management, accepted as the Croatian standard "HRN ISO/IEC 27000".
NATO	North Atlantic Treaty Organization.
NIAS	National identification and authentication system.
OIB	Personal identification number.
Strategy	National Cyber Security Strategy.