Pursuant to article 45, paragraph 1 of the Law on the Government ("Official Gazette of the RS" No 55/05, 71/05 – corrigendum, 101/07, 65/08, 16/11, 68/12 – CC, 72/12, 7/14 – УС и 44/14),

The Government hereby adopts the

STRATEGY

for the Development of Information Security in the Republic of Serbia for the period 2017-2020

"Official Gazette of the RS", No 53 dated 30 May 2017

1. INTRODUCTION

1.1. Information Security in the Republic of Serbia

Information security is an aspect of security related to the security risks associated with the use of information and communication technologies, including the security of data, devices, information systems, networks, organizations and individuals.

The development of new technologies brings undoubted benefits to society, but parallel with technological development come new security challenges. According to the Cybersecurity Strategy of the European Union, cybercrime is the fastest-growing type of crime, and millions of people, including children, are becoming victims of the attacks each day. Cyber attacks on information systems can significantly jeopardize the company's operations, functioning of state infrastructure and national security, while individuals, and above all children, are increasingly exposed to the risk of fraud, blackmail and abuse over the Internet.

The use of information and communication technologies (ICT) by the state, business sector and citizens is on the rise, and more and more tasks and activities are based on their use. State authorities rely heavily on information systems, which enable easier and more efficient performance of tasks within their jurisdiction. When it comes to relationship between authorities and parties, it should be noted that electronic government is developing, the number of public authorities' electronic services is increasing, enabling citizens to easily obtain various documents they need. Public enterprises performing activities of general interest, as well as companies, use the information systems to a large extent, and in certain activities, such as, for example, production, distribution and supply of electricity, the work relies heavily on ICT systems. Numerous institutions, such as, for example, institutions in the field of health care, keep records within their information systems. The use of the Internet is growing at all levels. According to the data of the Statistical Office of the Republic of Serbia, published in the document "Usage of Information and Communication Technologies in the Republic of Serbia, 2016", it was found that 99.8% of enterprises in the territory of the Republic of Serbia uses a computer in their business, 99.8% of enterprises has internet connection, and 99.1% has broadband internet connection. According to the same source, 98.6% of enterprises uses electronic public administration services. On the other hand, 65.8% of households owns a computer, 64.7% of households owns internet connection, and 57.8% of households in the Republic of Serbia has broadband internet connection. Also, over 1,510,000 persons use

electronic public administration services, and over 1,450,000 persons have purchased or ordered goods/services over the Internet in the past year.

Attacks on information systems can greatly jeopardize the functioning of the state, as was the case in Estonia in 2007, when cyber attack on ICT systems of state authorities and financial institutions was carried out, and when the e-government services, that are massively used in that country, were blocked, as well as payment transactions. Another known case is the introduction of computer virus "Stuxnet" into the nuclear power plant in Iran in 2010, in order to sabotage the industrial systems. In February 2016, hackers managed to steal $81 million from the Central Bank of Bangladesh by breaking into their computer network, discovering the keys to access the SWIFT system and issuing, without authorization, orders for funds transfer from the account at the Federal Reserve Bank of New York. In addition, there are threats to national security that, under international law, can not be classified as forms of armed aggression, but are present in international relations.

According to the data of the Ministry of Interior, the number of reported criminal offenses in the field of cybercrime is growing 50% annually. Attacks on state authority servers are more frequent and advanced.

The Republic of Serbia recognized information security as one of the six priority areas of the information society development, and took steps to establish a comprehensive information security framework. Accordingly, the Strategy for Development of the Information Society in the Republic of Serbia by 2020 ("Official Gazette of the RS" No 51/10) stipulates that the development and improvement of information security should be achieved through improvement of the legal and institutional framework, protection of critical information infrastructure, fight against cybercrime and scientific research.

The Law on Information Security ("Official Gazette of the RS", No 6/16 - hereinafter: the Law) created the basis for establishment and implementation of a comprehensive information security framework. The Law regulates protection measures against security risks in ICT systems of special importance, liability of operators of ICT systems of special importance in the management and use of ICT systems, and defines competent authorities for the implementation of protection measures, coordination between protection factors and monitoring of proper application of the prescribed protection measures.

In terms of establishing a comprehensive framework, the Law also leaves scope for involvement of other actors, such as private sector, academic community and civil society, by envisaging the creation of special working groups within the Body for the Coordination of Information Security.

Regarding the information security of individuals, children's safety is particularly important. The use of ICT and the Internet by children in the Republic of Serbia is very widespread. A UNICEF[1] survey conducted in 2012 on the territory of the Republic of Serbia showed that over 90% of older elementary and high school students has mobile phones, and that about 90% of

[1]*Popadic D, Kuzmanovic D, Utilization of digital technologies, risks, and incidence of digital violence among students in Serbia, UNICEF/Institute of psychology, Faculty of philosophy, University of Belgrade, 2012*

children uses the Internet. The same survey pointed out high rates of exposure to online risks and digital violence, i.e. two thirds of children have been exposed to some kind of online risk. At the same time, half of the interviewed teachers stated that they did not have the proper computer and internet skills, and almost half thought that they were not sufficiently informed about digital violence. According to 2016 UNICEF survey, "Survey about the level of awareness of parents who have children aged from 8 to 17 years about potential Internet risks and threats", only slightly more than 50 percent of parents consider themselves sufficiently, but not fully able to provide help and support to their child in such situations. The survey pointed out that 25 percent of parents stated that their child had been exposed to a risky or dangerous situation on the Internet in the last 12 months from the day of the survey. In addition, it noted that 85% of children aged from 8 to 17 years had a mobile phone, of which 63% were "smart phones", and that two out of three children spent an average of over an hour a day on the Internet.

The overall objective of the Strategy is to develop and improve information security in the Republic of Serbia and to maintain it at an adequate level. Given that the adopted regulations in this field define the ICT systems of special importance, the protection measures, and the competent authorities, the challenge to achieve the objective is to create preconditions for continuous staff development, both through introduction of special university programs in the field of information security, as well as through continuous training and development of employees in the relevant institutions dealing with information security. Taking into account the dynamics of this field, one of key preconditions for continuous maintenance of an adequate level of information security is the establishment of a center for development and research that would have the role to monitor the developments in this field and, consequently, to contribute to further improvement of information security in line with the latest knowledge and technological solutions. A stable functioning of the ICT system of special importance, the information security of citizens and the Republic of Serbia shall be achieved by realizing the objectives of the Strategy, the capacity to fight cybercrime shall be raised, but to do this, the cooperation between public sector, private sector, non-governmental organizations, academic community and other relevant factors is of key importance.

Considering the importance and scope of the information security field, the Government adopts this Strategy in order to develop and improve information security in the Republic of Serbia.

1.2. Information Security Regulatory Framework

The field of information security is regulated by the following regulations:

- Law on Information Security ("Official Gazette of the RS", No 6/16);
- Law on Organization and Jurisdiction of Government Authorities for Fight Against High Technological Crime ("Official Gazette of the RS", No 61/05 and 104/09);
- Criminal Code ("Official Gazette of the RS", No 85/05, 88/05 - corrigendum, 107/05 - corrigendum, 72/09, 111/09, 121/12, 104/13, 108/14 and 94/16);
- Law on Secrecy of Data ("Official Gazette", No 104/09);

- Law on Personal Data Protection (“Official Gazette of the RS”, No 97/08, 104/09 - as amended, 68/12 - CC and 107/12);
- Law on Electronic Communications (“Official Gazette of the RS”, No 44/10, 60/13 - CC and 62/14);
- Law on the Confirmation of the Convention on Cybercrime (“Official Gazette of the RS", No 19/09);
- Law on the Confirmation of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (“Official Gazette of the RS", No 19/09);
- Law on the Confirmation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (“Official Gazette of the RS - International Agreements”, No 1/10);
- Law on Military Security Agency and Military Intelligence Agency (“Official Gazette of the RS”, No 88/09, 55/12 - CC and 17/13).

2. PRINCIPLES OF INFORMATION SECURITY DEVELOPMENT

The development of information security in the Republic of Serbia is based on the following principles:

1) Information security is an integral part of overall security and it has the function of exercising and respecting the rights, freedoms and interests of the citizens, the business sector and the state;

2) Information security is important for all social factors using information and communication technologies, who need to be aware of the risks associated with the use of technology and to take preventive and other necessary protection measures;

3) Information security implies timely identification of risks, taking preventive measures and effective reaction to incidents;

4) It is necessary to establish and improve regular and efficient exchange of information on risks and incidents in the field of information security, at the national and international levels;

5) Maintain a continuous development of the protection system in information security at legal, organizational and technical levels, with adaptability to new circumstances and challenges;

6) Systematically raise awareness and improve knowledge and skills in all categories of citizens in terms of information security in everyday life and in the workplace;

7) Establish continuous cooperation between the public and the private sector as a basis for development and improvement of strategic priorities.

3. PRIORITY AREAS AND STRATEGIC OBJECTIVES

In order to develop and improve information security in the Republic of Serbia, the following priority areas shall be identified:

1) Security of information and communication systems, which refers to the risks of violating the functioning of government bodies, business sector and organizations as a result of incidents in information and communication systems;

2) Information security of citizens, which refers to the risks of violating citizens' security by the abuse of information and communication technologies;

3) The fight against cyber crime, which refers to the prevention and sanctioning of criminal offenses based on the abuse of information and communication technologies;

4) Information security of the Republic of Serbia, which refers to the risks of violating national security through information and communication systems;

5) International cooperation, which involves cooperation with foreign state bodies, international organizations and other partners in the field of information security.

Within the priority areas, the following strategic objectives shall be defined:

1) In the field of information and communication system security:

(1) prevention and protection by sharing information, monitoring current risks and raising awareness,

(2) security of ICT systems in business entities and security of e-commerce,

(3) security of ICT systems of special importance,

(4) security of classified data in ICT systems,

(5) cooperation between the public and the private sector in the field of information security;

2) in the field of citizen security in the use of technology:

(1) children's safety on the Internet,

(2) protection of privacy and protection against abuse in the use of ICT,

(3) information security in the education system;

3) in the field of fight against cyber crime:

(1) improving the mechanisms for detecting cyber crime and prosecuting the perpetrators,

(2) raising awareness of the dangers of cyber crime,

(3) promotion of international cooperation in the fight against cyber crime;

4) in the field of information security of the Republic of Serbia:

(1) information security system of importance for national security,

(2) development of scientific, technological and industrial capacities necessary for protection of information security of the Republic of Serbia,

(3) building military defense system capacities to defend against cyber attacks,

(4) building security and intelligence capacities in the field of information security,

5) international cooperation.

3.1. Security of information and communication systems

Information security incidents are usually associated with compromised security of information and communication systems, which can be a break into the system, access to data that should not have been enabled, causing problems in the system operation, and the like. The ultimate consequences of such incidents often go beyond the framework of the ICT system itself and are related to tasks, organizations and people who directly or indirectly rely on the ICT system. For example, the interruption to information system operation in a bank can prevent the bank from serving its clients, and it can result in a situation where the client can not pay the bill using their credit card. Such widespread incidents may jeopardize the functioning of the state, economy and society, which is why there are ICT systems of special importance defined, for which there is a legal obligation to provide information security, in accordance with the Law.

3.1.1. Exchange of information, monitoring current risks and raising awareness

In all spheres of security, new techniques and threats to security and new security measures are continually appearing, but in no other field this happens as dynamically as in information security.

This is why timely information, awareness raising, correction of habits and provision of relevant information on security risks and ways to eliminate consequences of incidents are of paramount importance.

Fast, reliable and efficient information exchange can influence public authorities, business entities and citizens to take timely and adequate measures to protect their systems and devices, thus preventing an incident to happen, or alleviating the consequences of an incident that has happened.

Therefore, the Law established the National Center for the Prevention of Security Risks in ICT Systems (National CERT) within the Regulatory Agency for Electronic Communications and Postal Services (RATEL), whose task is to collect and exchange information on the risks to the ICT systems security and the events that jeopardize the ICT systems security, and to inform, warn and advise, in this regard, the persons who manage ICT systems in the Republic of Serbia, as well as the public.

The National CERT should cooperate with similar organizations in other countries, given the global character of the challenges in the field of information security.

The National CERT should cooperate with relevant international institutions in the field of information security and participate as a member in their work.

It is of utmost importance to effectively establish and continually improve the work of the National CERT, in order for it to respond as much as possible to the given role.

Within the republic bodies, the Center for the Security of ICT Systems in the Republic Bodies (hereinafter: CERT of the republic bodies) within the Administration for Joint Services of the Republic Bodies was established by the Law, and it performs tasks related to the protection against incidents in the ICT systems of the republic bodies, except the ICT systems of independent operators. In addition, the Law has left the possibility of creating independent special CERTs that perform tasks of prevention and protection against security risks in the ICT systems within a certain legal entity, group of legal entities, business areas and the like. Special CERTs are registered with the National CERT. In this way, a CERT network should be established in order to exchange information and experiences efficiently and quickly.

3.1.2. Security of ICT systems in business entities and security of e-commerce

With the development of the electronic commerce, business entities are increasingly exposed to security risks associated with the technology they use.

First of all, business entities need to establish and improve the information security management systems in accordance with international standards and good practice from other countries.

In addition to CERT's activities aimed at raising awareness of, inter alia, business entities, it is necessary to set the improvement of the ICT system security in the economy as a special priority. Consequently, the significance of the National CERT is reflected in raising the awareness of business entities of the need to apply the protection measures in accordance with national and international standards, as well as of the benefits of setting up special CERTs (within a particular business entity, group of business entities or business areas) that should play an important role in the prevention and protection of ICT systems and the exchange of information with other relevant factors of the information security system in the Republic of Serbia. In order to raise awareness of the security risks and the importance of application of protection measures, the participation of non-governmental sector, academic community and other subjects in this field is of great importance.

3.1.3. Security of ICT systems of special importance

When the violation of security of a particular ICT system or several ICT systems in the same area may lead to significant disturbance of the functioning of public institutions, economy and everyday lives of citizens, then the responsibility for the safety of such an ICT system goes beyond the damage inflicted on an enterprise, organization or institution to which the ICT system belongs. These are the ICT systems critical infrastructure depends on, or systems that represent the critical infrastructure themselves. Since the concept of critical infrastructure has not yet been formally introduced in the legal system, such systems are designated as the ICT systems of special importance in the Law.

The operators of ICT systems of special importance have obligations established by the Law to take care of information security, and regarding this, they are under the supervision of the competent state bodies.

It is also stipulated that ICT systems of special importance shall inform the competent body whenever an incident, which may have a significant impact on violation of information

security, occurs in the ICT systems. The operators of ICT systems of special importance must be aware of the importance of reporting the incidents, as well as of their consequences at the national and international levels.

The competent body shall establish and promote international cooperation in the field of the ICT systems security, which will further formalize the accession of the Republic of Serbia to the European Union, based on the Directive on security of network and information systems of the European Union.

The competent body shall continuously monitor the state of information security through inspection supervision, reception and processing of notifications of incidents in ICT systems of special importance that can have a significant impact on violation of information security, as well as on the basis of the risk and incidents analysis developed by the National CERT, and in line with this, it shall improve the field of information security with cooperation of all relevant institutions, especially those whose representatives participate in the work of the Body for the Coordination of Information Security. Consequently, the capacity building of the competent body, that is the Ministry of Trade, Tourism and Telecommunications, is of utmost importance in terms of information security inspection and reception and processing of incident reports, as well as the capacity of other institutions in charge of information security.

On the other hand, the establishment of an information security management system, in line with the prescribed conditions, in a large number of the operators of the ICT systems of special importance is imminent, which is the ultimate purpose of legal measures and is of key importance for the security of critical infrastructure in the Republic of Serbia.

3.1.4. Security of classified data in the ICT systems

Classified data in the ICT systems are data that, in accordance with the rules on confidentiality of data, are determined and marked with a certain degree of confidentiality.

Protection of classified data in the ICT systems is a particular security challenge, bearing in mind that the most sophisticated forms of cyber attacks (including spyware) are precisely the attacks on the content of classified data.

Unauthorized access to classified data and their theft from the ICT systems of state institutions, public and private enterprises, as well as attacks on ICT infrastructure vital to the functioning of the state, can be viewed as one of the most severe forms of attack on the ICT system.

The Law on Secrecy of Data, and the bylaws adopted based on this Law, establish the basis for normative framework for dealing with classified data, including the issues of classified data processed in information and communication systems, as well as the competencies of the Office of the National Security Council and Classified Information Protection in this area. In the following period, the national regulations and competencies of the Office of the National Security Council and Classified Information Protection in the field of protection of classified information in ICT systems should be upgraded, in accordance with the relevant EU directives, with a special focus on determining the competencies and prescribing the process of accreditation of ICT systems for classified information.

The priorities in improving the security of classified data in the ICT systems are quick and efficient completion of establishment of uniform system and accreditation procedure for the ICT systems for classified information, defining the protection measures for ICT systems for classified information, adoption of national awareness-raising program for the use of ICT systems for classified information, and adoption of national methodology for risk assessment for ICT systems for classified information. To that end, it is necessary to further strengthen the capacities of the Office of the National Security Council and Classified Information Protection and other competent state bodies.

3.1.5. Cooperation between the public and the private sector in the field of information security

In order to maintain an adequate level of information security in the Republic of Serbia, the participation of others, in addition to that of the state, is necessary - of the business sector, citizens, non-governmental sector, academic community and other relevant factors. Cooperation between the public and the private sector can be very important for industrial research and innovation in the field of information security, and a very important segment of cooperation is the exchange of information in order to adequately prepare and respond to security risks and incidents.

The Law leaves room for involvement of actors from the private, academic and civil sectors in efforts aimed at strengthening information security in the Republic of Serbia by forming special working groups within the Body for the Coordination of Information Security. In this sense, the establishment of public and private sector cooperation that will enable efficient communication and optimization of planned future activities, i.e. timely exchange of information and sharing of resources, is also one of the starting priorities for the improvement of information security in the Republic of Serbia.

All these activities should lead to the establishment of permanent trust between all actors within information security framework: the public sector, i.e. the representatives of state institutions, the private sector, i.e. the business sector and citizens organized into civil society.

3.2. Security of citizens in the use of technology

In addition to the exposure of enterprises, organizations and public authorities to the risks to information security, every individual is exposed to these risks. Individuals may experience financial scams, damage to reputation for revealing intimate content, blackmail, damage due to loss of data, and particularly vulnerable category are children, who are, besides all this, often victims of abuse.

3.2.1. Children's safety on the Internet

Children increasingly use information and communication technologies and access to the Internet. By expanding the use of mobile devices, children can, at any time, without supervision of adults, gain access to the Internet, establish contact with strangers through social networks, expose too much personal information about themselves and their family, display individual and organized verbal aggression towards each other, record and share photos and videos that

may harm them or others. All these risks are taking place in the context of complex social relationships among children, including increasing peer violence.

By adopting the Law on Ratification of the United Nations Convention on the Rights of the Child ("Official Gazette of the SFRY - International Treaties", No 15/90 and "Official Gazette of the FRY - International Treaties", No 4/96 and 2/97), the state has committed itself to take measures to prevent and ensure protection of the child from all forms of domestic violence, violence in institutions and broader social environment. The provisions of the Convention stipulate that the states shall undertake measures relating to protection of the child from: physical and mental violence, abuse and neglect, and any other forms of exploitation harmful to any kind of child's well-being. Also, the Convention specifies the obligation of the state to provide support measures for physical and mental recovery of the child - victim of violence and its social reintegration.

The General Protocol for the Protection of Children against Abuse and Neglect, adopted by the Government in Conclusion 05, number 011-5196/2005 of 25 August 2005, provides that institutions and individuals from different systems (health, education, social protection, police, judiciary, etc.) should participate in the process of child protection against abuse and neglect, each within their jurisdiction.

The EU Strategy for a Better Internet for Children, adopted in 2012, stipulates that children, parents, guardians and teachers must be aware of the risks that exist on the Internet, and that children need to be advised and informed about safe ways of using the Internet. It points out that it is necessary to establish the mechanisms that will enable simple and easily accessible reporting of harmful and inappropriate content for children.

In July 2016, the Government adopted the Regulation on the safety and protection of children in the use of information and communication technologies ("Official Gazette of the RS", No 61/16). On the basis of this Regulation, the Ministry of Trade, Tourism and Telecommunications shall take preventive measures for the safety and protection of children on the Internet through information and education, and it has established the National Contact Center for Children's Safety on the Internet as a unique place for providing advice and receipt of complaints regarding the safety of children on the Internet.

The adequate protection of children on the Internet requires raising of awareness of both parents and children, as well as strengthening the role of the school through appropriate school programs and capacity-building of teachers. Public institutions that respond from different positions when it comes to certain consequences, such as the Ministry of Interior, centers for social work and health institutions, also need to build their capacities in this area.

It is also necessary to pay more attention to protection of children on the Internet in the media, through appropriate program contents, and thus contribute to raising the awareness of parents and children, which particularly applies to public media services.

It is necessary to further increase the capacity and strengthen the role of the unique place for providing advice and receipt of complaints regarding the safety of children on the Internet,

including coordination of support in individual cases and coordination of establishment of new system solutions for identified types of problems.

In cooperation of the relevant ministries with the electronic communications operators and the Academic Network of the Republic of Serbia, it is necessary to define the measures that will be able, at the technical level, to limit the exposure of children to inappropriate content.

3.2.2. Protection of privacy and protection against abuse in the use of ICT

The risks arising from excessive availability of personal data are often not sufficiently addressed by neither data owners nor processors, whereby the processors often intentionally disregard the need to protect personal data.

Most incidents in the field of information security, where an individual's security is threatened, include malicious collection of personal data, whether these data were obtained by fraud (the so-called "fishing" of personal data), breaking into a computer or other personal device, or by leaking data from databases.

It is necessary to further improve the legal framework in the field of personal data protection, in accordance with the standards of the European Union, as well as to remove the obstacles for more efficient implementation of the Law.

On the other hand, citizens need to significantly raise awareness of the importance of keeping their own personal data and not accepting excessive giving and publishing of personal data, as well as of possible frauds and other abuses on the Internet and of appropriate preventive measures.

3.2.3. Information security in the education system

"The mission of the education system in the Republic of Serbia in the 21st century is to secure the basic foundations of life and development of every individual, society and state based on knowledge."[2] In accordance with such defined mission, the Strategy for the Development of Education until 2020, as one of the goals of education development, aims to achieve and maintain the relevance of education, in accordance with immediate and developmental needs of individuals, economic, social, cultural, research, education, administrative and other systems.

The education system should ensure development and acquisition of general/interdisciplinary competencies of primary and secondary school students, relevant for personal, professional and social development and functioning of an individual in the modern world. The competencies defined in this way go beyond the framework of traditional school subjects and engage school knowledge in preparing the students to be competitive and functional in present and future educational and professional space, and to competently and actively realize their civic roles. One of the interdisciplinary competences is digital literacy: "The student is able to use available resources in the field of information and communication technologies (devices, software products, electronic communication services and services that are used by electronic communications) in a responsible and critical way, in order to effectively fulfill the set goals

[2]*Strategy for the Development of Education in Serbia until 2020 ("Official Gazette of the RS", No 107/12).*

and tasks in everyday life, education and future work. When using ICT, the student is aware of the risk to their own safety and well-being, and safety and well-being of others, and by acting responsibly, they protect themselves and others from unwanted consequences".[3]

The 21st century education mission and the orientation of educational process towards development of competencies have influenced the definition of strategic measures for the development of digital competences and the use of ICT. These measures primarily concern the improvement of the quality of conditions (defining the standards of school space and didactic, artistic and IT equipment, and defining the mechanisms for control of the application of these standards) and the quality of the teaching and learning process, which call for use of benefits of information and communication technologies and different forms of learning in the online environment (electronic conferences, subject blogs, discussion forums, electronic testing, etc.), and building the competencies of teachers to use information and communication technologies in teaching or class preparation, through initial education and teacher professional development system.

Due to the complexity of the issue of successful integration of ICT into the education system, as well as the fact that no documents have been prepared to help formulate educational policy in this area, the National Education Council (NPS) has initiated the development of a document Guidelines for improving the role of information and communication technologies in education (Guidelines).[4]

The guidelines provide an overview of all recommendations organized on the basis of two criteria: in relation to the level of generality and priority of implementation (high - emergency intervention, middle - start within one year and low priority in the period of three to five years). According to the criterion of generality, the recommendations are classified in relation to the level of: a) Development strategy: long-term planning, primary law adoption and monitoring of modern tendencies; b) Educational institutions: recommendations applied at the institutional level; and c) Teaching practice: recommendations relating to the immediate work of teachers.

Due to multifunctionality of the education system, a strong interdepartmental cooperation is needed in relation to the safety of children in the use of ICT (especially with the areas of safety, health and social policy). The departments, in the domains of their competences, should define and implement appropriate professional standards. At the national level, it is necessary to establish the functional coordination mechanisms between different systems and to clearly define their roles.

The education system should enable the acquisition of knowledge in the field of information security through introduction of special study programs at universities, which would contribute to the increase in the number of professional staff in this field, which is necessary, given the speed of ICT development and the increased risk of security incidents.

3.3. Fight against cyber crime

[3] *Standards of General Interdisciplinary Competencies for the End of Secondary Education, Institute for the Evaluation of the Quality of Education and Upbringing, Belgrade, 2013.*

[4] *Guidelines for improving the role of information and communication technologies in education, National Education Council of the Republic of Serbia, Belgrade 2013.*

Law on Organization and Jurisdiction of Government Authorities for Fight Against High Technological Crime, together with the provisions of the Criminal Code on criminal offenses of cyber crime, establish an institutional and legal basis for sanctioning of criminal offenses in this field. According to the Ministry of the Interior, 961 cyber crimes were detected in 2013, 1,423 such crimes were committed in 2014, and in 2015 this number significantly increased, amounting to 2,074, which in the right way illustrates the scope and the importance of preventing and combating this form of crime.

3.3.1. Improving the mechanisms for detecting cyber crime and prosecuting the perpetrators

In order to effectively combat cyber crime, it is necessary to improve the existing legislative framework. In 2009, the Republic of Serbia adopted the Law on the Confirmation of the Convention on Cybercrime CETC 185 (Budapest Convention) and the Law on the Confirmation of the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, while in 2010 the Law on the Confirmation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse was adopted.

However, the Republic of Serbia has not yet fully aligned its legislation with the Directive 2013/40/EU on attacks against information systems, which is one of the mechanisms for detecting and prosecuting perpetrators of criminal offenses in this field.

Evolution of the method of cybercrime execution follows the development of information technologies. This is one of the forms of crime with the highest growth rate, given that every day more than a million people around the world become victims of the crime. For this reason, the competent state bodies - Specialized organizational cybercrime unit within the Ministry of Interior and the Special Prosecutor's Office for Cybercrime must improve their operational tools and operational capability for suppressing this type of criminal offense. Also, it is necessary to improve the coordination and common approach of investigative authorities, prosecution authorities, public and private sectors.

In addition, it is necessary to continue the implementation of training of judges for dealing with these cases, bearing in mind the accelerated development of modern information technologies, as well as the new ways of committing the criminal offenses of cybercrime.

3.3.2. Raising awareness of the dangers of cybercrime

The end users play a key role in ensuring the security of networks and information systems, and therefore they must be aware of the risks they face online, and prepared to take simple steps to prevent the risky situations.

In that sense, it is necessary for public bodies, public and private sectors to organize public campaigns on the most common forms of cybercrime, such as unauthorized access to computer or computer network, security threats, Internet frauds, abuse of payment cards, and campaigns and workshops focused on the safety of children on the Internet, primarily regarding digital violence and sexual exploitation.

3.3.3. Promotion of international cooperation in the fight against cybercrime

Bearing in mind that cybercrime, due to the global reach of the Internet, knows no boundaries, it is extremely important to further improve international cooperation with the relevant foreign countries bodies. The Republic of Serbia, as one of the signatories of the Budapest Convention, has a remarkable role in the work of the 24/7 contact point network, established under the Convention, with two representatives for cooperation and urgent action in cases in this field. One contact point is the Special Prosecutor for Cybercrime, and another is a representative of the Cybercrime Unit of the Ministry of Interior.

3.4. Information security of the Republic of Serbia

Information security of the Republic of Serbia is a key part of a comprehensive national security, based on the information security of institutions, forces, people, systems, processes, information and values that are important for the security and defense of the country.

The information and communication infrastructure, and the defense system services and data have a special significance for the national security of the Republic of Serbia. Therefore, the information security of the defense system is one of the key components of information security in the Republic of Serbia.

3.4.1. Information security system of importance for national security

In the Republic of Serbia, it is necessary to define an information security system of importance for national security, in accordance with the existing competencies and additional defined roles of state and other bodies.

3.4.2. Development of scientific, technological and industrial capacities necessary for protection of information security of the Republic of Serbia

Information security in the function of defense of the Republic of Serbia is based on organized knowledge management in the field of information security, and management of people as bearers of this knowledge. Therefore, the basic task of development of the information security system is building, development and investment in the education system, trainings, research and development and investing in people as knowledge bearers in the area of information security in the field of defense. This involves jointly proposing, adopting and implementing the standards and practices that increase safety and security. Cooperation of the academic community with the relevant institutions, with the active participation of the private sector, should be institutionalized in order to jointly undertake certain activities for development of products, processes and services in order to prevent and provide an adequate level of information security. The academic community, on one hand, and the private sector on the other, using their expertise, will point to examples of good practice by emphasizing the importance of risk and management analysis in organizations through the organization of appropriate trainings, seminars, forums. Education of professional staff will enable the establishment of safe IT solutions available to users.

Through joint projects with the public and private sector, the academic community will contribute to continuous improvement of methods for identifying and determining security problems, implementation of adequate control, establishment of effective communication among all stakeholders and exchange of information on best practices in other countries.

Encouraging the cooperation between the scientific community and the economy, with clearly defined information security needs, will contribute to the development of technologies and services in accordance with accepted international standards. Taking the measures, which will contribute to preservation of information security in the Republic of Serbia, by all relevant subjects, will lead to improvement of the situation in this area. Launching the experimental environments for development of new technologies and services at universities will contribute to development of new solutions that will be used to respond to the growing number of challenges in the field of information security.

3.4.3. Building military defense system capacities to defend against cyber attacks

The Ministry of Defense and the Serbian Armed Forces will develop comprehensive capabilities for defense in the cyber space, in accordance with the constitutional and legal competencies and assigned missions and tasks. These activities include the establishment of information security and the ability to perform defense in the cyber space, within the effective use of forces and functional capabilities of the Serbian Armed Forces as the main subject of the defense system.

The Ministry of Defense and the Serbian Armed Forces are defenders against threats from the information space of all systems and resources in their jurisdiction in such a way that fully enables safe and reliable use of these systems and resources in order to perform the assigned competencies, missions and tasks.

It is particularly important to predict the obligations of the defense system subjects in the protection of the ICT systems in the state of emergency and war. It is also important to predict the engagement of the forces of the Ministry of Defense and the Serbian Armed Forces in providing assistance to the operators of the ICT system of particular importance, in terms of detecting the threats and adequate response with the aim of defending them and preventing the threats to national security of the Republic of Serbia.

3.4.4. Building security and intelligence capacities in the field of information security

The Security Services of the Republic of Serbia will develop comprehensive capabilities to protect the information security of the Republic of Serbia in accordance with the legal competencies, in order to protect the ICT systems of special importance, in terms of timely detection of threats, with the aim of preventing the threats to national security of the Republic of Serbia.

3.5. International cooperation

The widespread interconnection of social, organizational, technical, financial, economic and other types of systems across national borders, based on the use of ICT and systems, creates a complex international environment in which dynamic interaction between diverse subjects takes place. Social and economic prosperity, national security and defense of the Republic of Serbia directly and indirectly depend on the ICT networks that extend within and outside the national borders in a complex, dynamic and often unpredictable environment. ICT-based interaction is a two-way interaction, and it has complex direct and indirect impact on national

security. This impact must also be regulated in a complex way, through various forms and contents of cooperation at the national and international levels.

The establishment and development of information security at the national level can be achieved only through the implementation of a comprehensive set of activities simultaneously implemented and coordinated at the national and international level. Contact with the international partners is multilayered, active and optimal, as it includes a wide range of governmental, non-governmental and supranational organizations at the political, technical and professional levels.

The key international partners of the Republic of Serbia in this respect are the United Nations (UN), the Organization for Security and Co-operation in Europe (OSCE), the European Union (EU), the Council of Europe (CoE), the political, economic, security and defense organizations and alliances Serbia has concluded agreements on mutual cooperation with, neighboring and traditional allies of the Republic of Serbia.

In order to achieve the set international cooperation goals of the Republic of Serbia, it is necessary to establish and develop international cooperation on bilateral and multilateral basis, with the aim of improving the national and international information security. In addition, it is necessary to establish cooperation in order to exchange information, knowledge and experience with foreign network of national, professional and international centers for the prevention of security risks in the ICT systems. If possible, the Republic of Serbia should actively participate in international civil and military exercises aimed at establishing and developing the information security at all levels.

4. STRATEGY IMPLEMENTATION

The implementation of this Strategy is monitored by the Ministry of Trade, Tourism and Telecommunications.

The Government will adopt the Action Plan for the implementation of this Strategy within six months of its publication in the “Official Gazette of the Republic of Serbia”.

5. FINAL PART

This Strategy shall be published in the “Official Gazette of the Republic of Serbia”.

05 number 030-3942/2017-1

In Belgrade, on 29 May 2017

Government

President,

Aleksandar Vučić, sgd.