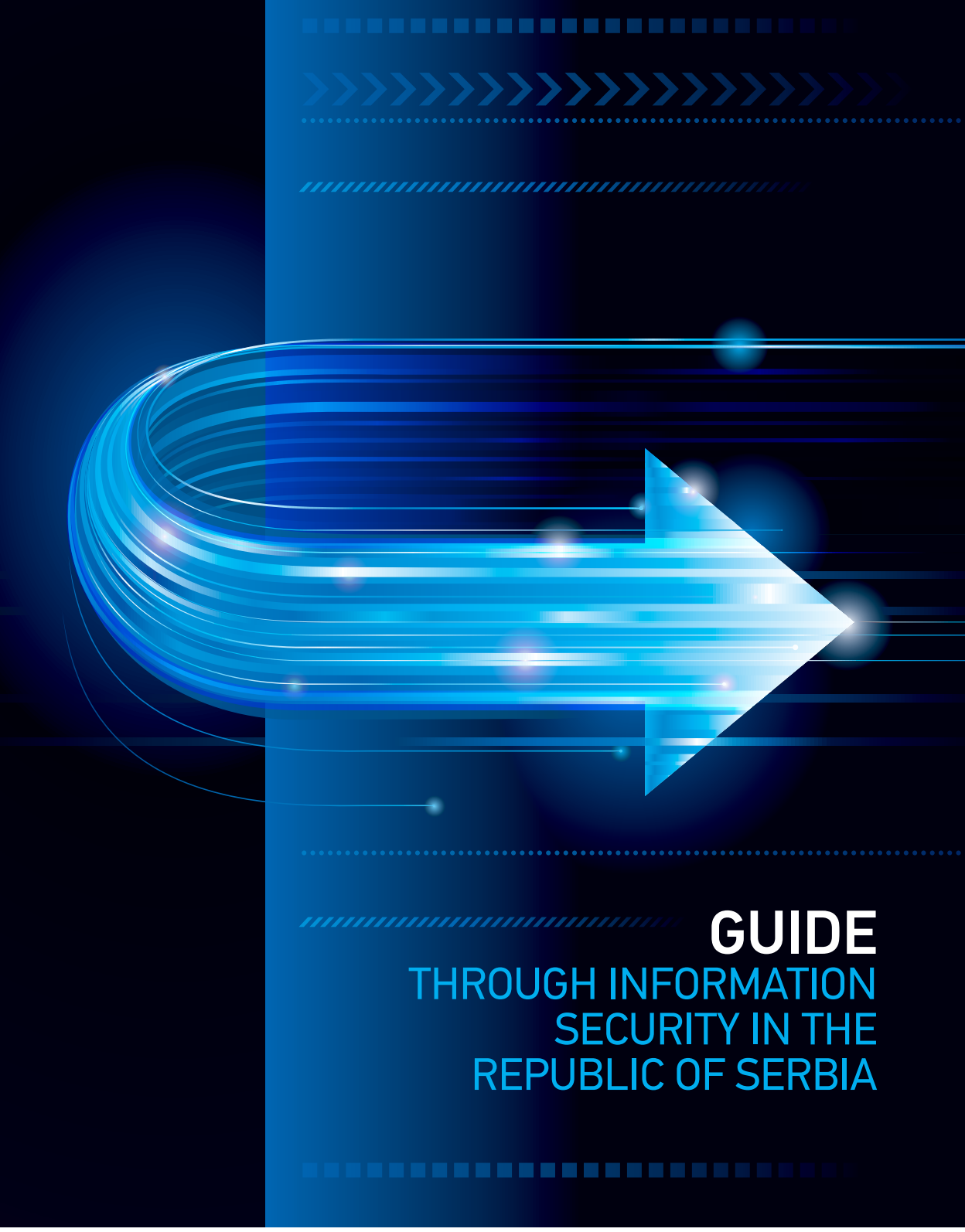

GUIDE
THROUGH INFORMATION SECURITY IN THE REPUBLIC OF SERBIA

OSCE Organization for Security and Co-operation in Europe
Mission to Serbia

Guide through Information Security
in the Republic of Serbia

GUIDE
THROUGH INFORMATION SECURITY IN THE REPUBLIC OF SERBIA

Authors:
Irina Rizmal
Vladimir Radunović
Đorđe Krivokapić

Title:
Guide through information security in the Republic of Serbia

Publishers:
Centre for Euro-Atlantic Studies – CEAS
OSCE Mission to Serbia

Design and prepress:
comma | communications design

Print:
Grid studio

Copies:
100

Content

Content

Content

LIST OF ACRONYMS

APTs	Advanced Persistent Threats
CBMs	Confidence Building Measures
CCD CoE	NATO Cooperative Cyber Defence Centre of Excellence
CEME	Compromising Electromagnetic Emanations
CERT/CIRT/CSIRT	Computer Emergency Response Team
CI	Critical infrastructure
CII	Critical information infrastructure
CIWIN	Critical Infrastructure Warning Information Network
DIBS	Society for Information Security Serbia
DIS	Informatics Association of Serbia
EDA	European Defence Agency
EEA	European Economic Area

LIST OF ACRONYMS

EFSI	European Fund for Strategic Investments
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
EP3R	European Public-private Partnership for Resilience
ESOs	European Standardisation Organizations
EU CFSP	Common Foreign and Security Policy
FP7	EU's Seventh Framework Programme for Research
GCA	ITU Global Security Agenda
GSP	Microsoft Government Security Program
IcSP	Instrument contributing to Stability and Peace
ICT	Information and Communications Technologies
IMPACT	International Multilateral Partnership Against Cyber Threats

LIST OF ACRONYMS

IoT	Internet of Things
IPA	Instrument for Pre-accession Assistance
IPAP	Individual Partnership Action Plan
ITU	International Telecommunications Union
NICP	NATO Industry Cyber Partnership
NIS	Network and Information Security
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Cooperation in Europe
PARP	NATO Planning and Review Process
PKS	Chamber of Commerce and Industry of Serbia

LIST OF ACRONYMS

RATEL	Regulatory Agency for Electronic Communications and Postal Services
RNIDS	Serbian National Internet Domain Registry
RIS3	Research and innovation strategies for smart specialisation
S3 Platform	European Commission Smart Specialisation Platform
SPS	NATO Science for Peace and Security Programme
UNCTAD	UN Conference on Trade and Development
UN GGE	UN Group of Governmental Experts
UNODC	UN Office for Drugs and Crime

SUMMARY

Guide through Information Security in the Republic of Serbia is a study compiled by the Centre for Euro-Atlantic Studies from Belgrade (CEAS) within the project *Serbia Moving Forward: Mapping the Legal and Policy Cyber Security Framework*, supported by the OSCE Mission to Serbia. The objective of the Study is to point out to the obligations arising from Serbian membership and participation in international bodies and organizations, but also to the potential of such membership, following the recent adoption of the first Law on Information Security in the Republic of Serbia in January 2016. The Study is focused on the existing regulatory framework, strategies, principles and recommendations issued by the bodies such as the European Union, NATO, Organization for Security and Cooperation in Europe and the United Nations. The Study also provides basic guidelines for further steps in the process of comprehensive regulation of the area of information security in Serbia, such as the development of the Strategy for the Development of Information Security, as well as of the bylaws that are expected to be adopted and that will regulate certain areas covered by the Law in greater detail. In that sense, the Study is intended for decision makers, i.e. for representatives of the relevant state institutions, as support to efforts directed at regulation of the area of information security in Serbia, but also for representatives of the private sector, academic community and civil society interested in this field.

Research for the purpose of this Study was conducted from May until August 2016. It was based on an analysis of publicly available literature, materials and official documents on this subject, as well as consultations with representatives of the Ministry of Interior, Ministry of Defence, Office of the National Security Council and Classified Information Protection and the industry. The Study was compiled by a team of authors led by Irina Rizmal, Senior Project Coordinator of the Centre for Euro-Atlantic Studies, together with Vladimir Radunović, Director of the Cyber Security Program and e-Diplomacy of DiploFoundation and Đorđe Krivokapić, Program Director of the SHARE Foundation. Additional support to the team of authors was provided by Danilo Krivokapić and Andrej Petrovski also from the SHARE Foundation.

All the obligations, principles, standards, recommendations and guidelines cited in the Study are based on cross-checking of existing regulatory and technical frameworks, as well as on the basis of already developed mechanisms and guidelines for comprehensive regulation of national information security and international efforts in this field.

Bearing in mind the fact that Serbia is at the very beginning of developing a comprehensive approach to the area of information security, this Guide is primarily intended to provide an overview of issues of the initial regulation of this field, primarily from the regulatory aspect. In addition to concrete recommendations for the basic regulation of national

information security, the Study opens some questions related to the national information security building process, such as critical infrastructure; the relationship between the state, service providers and end users (citizens); awareness raising and education and building of trust and mechanisms of public-private partnership in this field, etc. In the long term, these and other important question, which had to be omitted in this Study due to objective restrictions related to length, such as the need for a national body in charge of information security, issues pertaining to online freedoms, intellectual property protection in cyber space, are all issues deserving individual analysis.

The first Chapter provides an insight into the significance of cyber security on the global level and its position in international bodies and organizations, but also into the situation in the Republic of Serbia following the adoption of the Law on Information Security. The second Chapter analyses the principles and standards adopted in Serbia through the strategic orientation on the international level in terms of membership in the European Union, Organization for Security and Cooperation in Europe, United Nations and its cooperation with NATO. The third Chapter comprises a brief analysis of the adopted Law on Information Security, the significance of the existence of an umbrella document, perceived deficiencies and possible mechanisms for overcoming some of these deficiencies in the short term. The fourth Chapter is focused on the forthcoming step of adoption of the Strategy for the Development of Information Security and provides basic guidelines that pertain to certain principles and models that may be introduced through the Strategy in the area of information security in Serbia, such as risk assessment, standardisation, optimization through public-private partnership and evaluation, as recommended by international organizations and bodies. The fifth Chapter maps out the possibilities made available to Serbia through the aforementioned strategic orientation on the international level, in terms of program-related financial resources and training programs focused on the development of knowledge and capacities in the area of information security. The sixth Chapter is in its entirety dedicated to the issue of establishing public-private partnerships in the area of information security, while pointing to the fact that this concept is becoming a standard on the international level, and develops three possible scenarios for developing such mechanisms. The seventh Chapter points to different development models of certain elements of information security in the short, medium and long term, depending on what Serbia will define as strategic priorities in this field. The final, eighth Chapter contains a basic list of legal regulations related to the newly adopted Law on Information Security and the amendments and addenda of these, that should be considered in order to achieve harmonization of the entire national regulatory framework.

A special note pertains to the terminology used in the Study, i.e. to the overlapping of the terms “information security” and “cyber security”. Due to the fact that the debate on the use

of these two terms is still ongoing on the international level too[1], without attaching primacy to one or the other term, the team of authors decided to use the term "information security" when conducting analysis of the regulatory framework of the Republic of Serbia, since the term is used in official state documents, while the term "cyber security" is used in its source form in which it is found in international documents.

1 While the term "information security" is used in expert circles in the context of protection of confidentiality, integrity and availability of information, and the term "cyber security" includes both the protection of networks and infrastructure, as well as the protection of users, the Euro-Atlantic block of countries uses the term "cyber security" in global political debates as a broader concept of protection from cyber attacks while maintaining an open and free cyber space, while the countries of the Shanghai Cooperation Organization (most notably Russia and China) use the term "information security" as a broader concept that additionally includes threats in the form of information war and propaganda.

I INTRODUCTION AND GENERAL CONTEXT

The Internet is often defined as a network of all (computer) networks. Cyberspace, however, includes both the elements of technology and of society, and represents a complete, complex environment made up of hardware and software networks, data and systems, infrastructure and services, business, as well as people and their communication. The Internet is an integral part of the everyday life of modern society: communications, business, trade, education, culture, healthcare systems, diplomacy, security systems, critical infrastructures, traffic, but also entertainment and social interaction, as well as "traditional business activities" such as agriculture, are increasingly benefitting from Internet services. There are also the technologies such as virtual reality and the "Internet of things" (IoT), in which objects such as light bulbs, vehicles, traffic lights, buildings and power plants, communicate among themselves while creating a "smart", interactive environment, while artificial intelligence and "smart" implants connected to the Internet are the near future. Owing to the integration of the Internet in all segments of society, cyberspace is becoming the key component of our real life environment.

Despite its numerous advantages and huge potential, the Internet is used for malicious activities as well – over the past years, some of these led to substantial financial losses and even to the destruction of property and loss of life. Due to the key role that the Internet plays in today's society, risks for the economy, human freedoms and security are increasing: from the potential attacks on the Internet infrastructure, and thus the disabling of all cyber space services, including the financial sector and critical infrastructure such as the electric grid or water supply network, to interception of information and communications and abuse of private and confidential data. Some authors claim that, just like other domains of security, the security challenges in cyber space are no longer imminent, direct or certain like before, but are becoming indirect, unintended, uncertain, and situated in the future, since they only materialize when they actually take place[2]. In the future not so far ahead, however, risks could reach the limit of socially acceptable ones, which could affect the levels of trust in the entire cyber space, and shake up the social contract itself as the foundation of the society of today[3].

2 E. M. Brunner, and M. Suter. 2008. International CIIP Handbook 2008/2009. Center for Security Studies. ETH Zurich. http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf.

3 J. Kurbalija. 2015. In the Internet we trust: Is there a need for an Internet social contract?. DiploFoundation blog. http://www.diplomacy.edu/blog/internet-we-trust-there-need-internet-social-contract.

This is why the Internet carries global, as well as strategic importance for each individual country. Internet governance, as well as the security of the entire cyber space came into focus of national and global policies due to the geostrategic importance of cables and connections, digital data flow and control, management of resources such as Internet domains and unique numbers (the so-called "IP addresses"), as well as due to the creation of new standards that will define the functioning of society in the near future. Cyber security thus found itself at the top of the diplomatic and political agenda of the European Union, Council of Europe, NATO, United Nations, Organization for Security and Cooperation in Europe (OSCE), G8 – Group of the most developed economies in the world, the International Telecommunications Union (ITU) and other important international bodies and groups. Cyber space has become the space for potential war waging, and thus cyber defence has been categorized among the principles of collective defence within NATO[4] and the EU[5], or more precisely, as an additional, new dimension of war waging, along with waging war on land, in the air, and at sea, and, among some actors, in space as well. Police forces and judiciaries are working increasingly hard on the national level, and through international cooperation as well, to suppress cybercrime, which is becoming a part of the everyday experiences of citizens and institutions. Discussions on the protection of critical information infrastructure and combating cyber terrorism are in their initial stages.

At the same time, cyber attacks themselves have become omnipresent and more sophisticated, and the tools used for such attacks have become available to a broader circle of interested parties: from hackers (both "good" and "bad" ones) and political activists, through criminal groups and terrorists, to security structures and national armed forces. To make matters even more complex, taken independently, national authorities do not have the substantial power required for developing cyber security, since the majority of Internet infrastructure is owned by private companies, which are situated all over the world and within different jurisdictions, while the expertise and relevant international contacts can mostly be found among the academic, technical and civil society communities.

A comprehensive and systematic approach that includes various actors is the foundation of the response to cyber security risks, but also to the exploitation of economic and developmental potentials that the Internet, and the cyber security industry as well, can offer. The multidisciplinary character of the field of cyber security requires actors that are familiar with different subject matters, such as the technology, law, psychology, sociology, economics, politics and diplomacy, among others. A broad public-private partnership enables each actor to contribute to cyber security: state authorities and regulatory bodies through creation of the legal, regulatory and political framework; police, prosecution and judiciary authorities through combating high-tech crime (HTC) and strengthening of mechanisms for international cooperation; private sector and technical communities through expertise and experience and through de-facto control over the majority part of the infrastructure, services and standards; civil society and the academic sector through knowledge,

4 Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers. 14.6.2016. NATO. http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

5 Cyber Defence. 4.6.2015. European Defence Agency. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

networks of contacts and capacity to reach the end users, as well as to warn against potential violations of human rights.

Many countries have adopted relevant legal frameworks (mostly by taking into account both security and human rights), as well as national strategies for cyber security. A large number of countries have already established the operational mechanisms that enable them to react to cyber incidents and to coordinate issues of cyber security, which include both, representatives of the state authorities, as well as representatives of expert and academic communities, the private sector, operators of critical infrastructure (providers of essential services) and the civil society.

State of affairs in the Republic of Serbia

The Republic of Serbia (hereinafter: Serbia), like many other countries in the Western Balkans, is lagging behind in these fields. Most of the countries in the neighbouring region, with the exception of Bosnia and Herzegovina and Macedonia, have at least taken the initial steps towards establishing the legal framework, primarily by following the guidelines issued by the European Union, a member of which they are striving to become; and yet, most of them lack a comprehensive strategic approach, efficient operational mechanisms, as well as multi-actor cooperation[6]. At the same time, the risks for Serbia and the countries in this region are the same as those in other countries, which is corroborated by the growing number of incidents, such as the hacking of official institutions and media after an incident at a football match between the national teams of the Republic of Serbia and Albania, leakage of private data of millions of citizens due to an omission in the work of the Privatization Agency, or forgery of an e-mail message of a high official from the Ministry of Interior.

Since May 2014, the SHARE Foundation has been constantly monitoring the situation in the field of digital rights and freedoms in Serbia and has recorded the cases that are dubious from the aspect of the right to freedom of expression and right to information, right to privacy, digital safety, as well as other rights of individuals that can potentially be jeopardized online. According to the methodology used for recording such cases from the above mentioned date and until the conclusion of this Study, the SHARE Foundation recorded a total of 45 cases of technical assaults on integrity of content, or, more specifically 29 cases where the content was made unavailable, 5 cases in which data and programs were destroyed and stolen, and 11 cases of unauthorized access, i.e. unauthorized modification and uploading of content.

The most significant infamous incident undermining information security in the Republic of Serbia was identified in late 2014. Namely, that November, a link towards a

6 Group of authors. 2016. Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. DiploFoundation. (Restricted availability)

file of more than 19 GBs became viral via social networks, containing more than 4,000 financial documents and endless lists of individuals containing their personal data. The size of the textual part of the file slightly exceeded one gigabyte and contained data on exactly 5,190,396 citizens of Serbia, i.e. data from the records on the holders of the right to free shares held by the Privatisation Agency, and specifically the names, surnames, middle names and Unique Citizen Identification Numbers. Following supervision conducted by the Commissioner for Information of Public Importance and Personal Data Protection, it was determined that the document was publicly available since February 2014 and that it was downloaded "for a number times".

According to estimates from 2013, a comprehensive cyber attack on Serbia, disabling the key segments of society, such as the state administration, telecommunications and the banking sector, would incur damage exceeding 10 million Euros per each day of such an attack, with significantly higher losses if the attack was to last for several days.[7] With the imminent increase of digitalization of society, including e-services of the state administration and integrated databases on citizens, e-healthcare, the linking of critical infrastructure and industry, and integrated digital systems of the financial sector and banks, the stakes, i.e., the risks are ever higher.

In early 2016, Serbia adopted the Law on Information Security, through which, in addition to the existing legislative framework through which the provisions of the Council of Europe Budapest Convention on Cybercrime are implemented, the fundamental legal framework in this area was established. The adoption of the Law on Information Security was additionally envisaged within the Serbia's process of accession negotiations with the EU, in the National Program for the Adoption of the EU Acquis (NPAA) for 2014-2018[8], as well as in the Strategy for the Development of Information Society in the Republic of Serbia by 2020[9].

In itself, the adopted Law is an important step for Serbia, although some important issues are resolved in an incompetent and/or dysfunctional manner. The bylaws will therefore be of key importance for a sound and efficient legislative framework, but due to the nature of this topic and specificity of cyber space, it is important to have these shaped through full cooperation with all the stakeholders and relevant actors.

Serbia lacks a comprehensive national strategy for the development of information security that would, just like the Strategy of the European Union and other sound strategies, serve as the basis for establishing of the entire regulatory and operational environment. The Strategy should define the key directions and objectives of activities in the field of information security, as well as recognize the importance of a multi-partner model and public-private partnership, encourage communication among different actors and sectors and provide for a transparent process of its implementation in order to establish trust among

7 V. Radunović. 2013. DDoS - Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR).

8 National Program for the Adoption of the EU Acquis. July 2014. Serbian European Integration Office. http://www.seio.gov.rs/upload/documents/nacionalna_dokumenta/npaa/npaa_2014_2018.pdf

9 Strategy for the Development of Information Society in the Republic of Serbia by 2020. Official Gazette of the RS, No. 51/2010.

the actors. Bearing in mind good practices from other countries, the strategic framework should, in addition to the security of society and citizens, take into account the respect of human rights, define the area of critical infrastructure protection along with the role of education on all the levels, but also acknowledge the potential that digital society, as well as cyber security, offer for development and the economy.[10]

Concerning the operational mechanisms, Serbia has in place the Service for Combating High-Tech Crime (HTC) within the Ministry of Interior, as well as a special Department of the Higher Public Prosecutor's Office in Belgrade for the territory of Serbia, while on the level of judiciary specific jurisdiction for HTC was defined through the special department of the Higher Court in the first instance, i.e. through the special department of the Court of Appeal in Belgrade in the second instance.

In addition to that, the Law on Information Security envisages the establishment of a national Computer Emergency Response Team (CERT)[11], within the Regulatory Agency for Electronic Communications and Postal Services (RATEL).

A serious deficiency in the existing legislative framework is an insufficiently defined space for public-private partnership. The Law envisions the establishment of a Body for the Coordination of Information Security (which was established by means of the Decision on Establishing of the Body for the Coordination of Information Security from March 8, 2016[12], hereinafter: the Coordination Body), but it provides that only representatives of several state institutions should be included as its members, primarily representatives of the competent Ministry – the Ministry of Trade, Tourism and Telecommunications (MTTT) – as well as representatives of the Ministries of Defence, Interior and Foreign Affairs, representatives of the security services, as well as of the national CERT, while leaving out representatives of the Ministries in charge of economy, education and culture, as well as representatives of the private, academic and civil sectors. The Law indeed envisaged potential establishment of expert working groups within the Coordination Body, but this remains on the level of a possibility, whereby the groups are to be formed on a needs-based approach, for specific, concrete issues.

Public-private partnership, as a model, has not yet been applied in starting up the Internet industry or the cyber industry, education or in activities directed at awareness raising, with the exception of, to a limited degree, the level of campaigns for online child protection.

However, initiatives launched by several actors in the field of cyber security in Serbia over the past years managed to achieve visibility. In January 2015, Serbia took over the OSCE

10 Such a strategic framework is one of the guidelines arising from the project implemented by the Diplo Centre and the OSCE Mission to Serbia in mid-2015. Detailed information is available in the final publication of this project: Towards the National Framework for Cybersecurity in Serbia (*Ka nacionalnom okviru za sajber-bezbednost u Srbiji*). 2015. Diplo Centar. https://issuu.com/diplo/docs/ka_nacionalnom_okviru_za_sajber-bez.

11 Both the terms CIRT and CSIRT are used in international documents: Computer (Security) Incident Response Team. In this document, we shall predominantly use the term CERT.

12 Decision on Establishing of the Coordination Body for the tasks related to information security. Official Gazette of the RS, No. 24/2016. 1003.

Chairmanship, and it kept cyber security among the leading topics on its chairmanship agenda, which was set as one of the priorities by the previous Chair, Switzerland. In this regard, in October 2015, a special event was organized under the auspices of the OSCE Chair (Republic of Serbia) on the subject of effective strategies for cyber security and ICT risks, in which representatives of OSCE countries gathered and, in addition to formal discussions, its program included a simulation of a multi-actor dialogue in case of a cyber conflict between two countries. The Diplo Centre, with the support of the OSCE Mission to Serbia, organized a series of workshops for representatives of all the key institutions, private sector and civil society dedicated to discussions on cyber security in Serbia in general, as well as the development of a national strategic framework for cyber security, while the Geneva Centre for Democratic Control of Armed Forces (DCAF) organized a public hearing on cyber security in the Republic of Serbia during the process of adoption of the Law. The Serbian National Internet Domain Registry (*Registar nacionalnog Internet domena Srbije*, RNIDS), Informatics Association of Serbia (*Društvo za informatiku Srbije*, DIS), Society for Information Security (*Društvo za informacionu bezbednost*, DIBS), Serbian Chamber of Commerce and Industry (*Privredna komora Srbije*, PKS) and other organizations have, on several occasions, organized public discussions and expert conferences on cyber security, and the Faculty of Organizational Sciences of the University of Belgrade established a partnership for the purpose of preparing an application for the *Horizon2020* funds of the European Union program for supporting the development of CERTs, which was, unfortunately, unsuccessful.

In addition to these projects, directly related to cyber security policies in Serbia, a large number of conferences and public discussions were organized on specific aspects of this field, such as child protection. In this sense, the only larger public-private partnership was created in the form of the Safer Internet Centre and the *Click Safely* campaign that included the competent Ministry, operators of telecommunications services and other actors, and afterwards the Fund B92 Foundation as well; their *Net Patrol* Project[13] for reporting of illegal and harmful online contents which formally still exists, although there is no relevant data on the use of this service.

In addition to that, a number of private and sectorial CERTs are in the initial stages of development: the CERT of the Ministry of Interior, aimed at protecting the systems and data related to activities performed by the MoI, became operational in 2015, while it is expected that the CERTs of RNIDS, aimed at protecting the national domain space, of the SHARE Foundation, aimed at providing support to organizations and media under cyber attacks, as well as those of a group of Internet operators, will be established in the future period.

Finally, the topics related to the protection of critical infrastructure, or those related to education and building of national competencies in the field of cyber security, have not yet been opened in Serbia. Critical infrastructure, and in particular, critical information infrastructure, have not yet been clearly defined by law, and their protection will probably be defined within the bylaws related to the Law on Information Security. The dialogue among state authorities, expert organizations, the private sector, the national CERT and critical

13 Net Patrol. http://www.netpatrola.rs/sr/naslovna.1.1.html.

infrastructure operators – among which a growing number of private entities, in particular in the area of energy – has not yet been initiated, despite the alarming news from other countries about the serious consequences of the cyber attacks on the electrical power system, steelworks, and the like.[14]

In regard to education, in mid-2016 the National Council for Education rejected the proposal pertaining to the introduction of computer science as a mandatory subject in primary schools, whereby a good method of formal introduction of the topic of cyber security in the education system – including the culture of online safety – was thwarted. In addition to that, there are no academic multidisciplinary programs that could provide for capacity building in this field in the long term and transform the workforce towards jobs in the field of cyber security – both in the systems for defence from attacks, as well as in policy building systems, or the potential commercial industry and the start-up sector – nor are there any specialized programs that could enable the leadership level in key institutions and companies, to understand the risks and prepare the systems for the increasingly sophisticated and dubious cyber attacks in a faster and more efficient manner. It is in these areas that Serbia should invest serious efforts, primarily through its future strategic framework. A potential step forward in this area is the announcement from the exposé of the Prime Minister of the Republic of Serbia, Aleksandar Vučić, according to which, over the following years, computer science will be introduced in the curriculum for primary school, following the model of EU and Scandinavian countries, along with the development of specialist programs for technical dual education.[15]

The building process of the operational and legal framework for cyber security does not end with the establishment of the CERT, or with the adoption of laws and a strategy. These are in fact only the initial steps and a good basis for a safe national cyber space. A lot can be done through initiatives of public-private partnership, where the recommendations, experiences and good practices of the international organizations and other countries can serve as excellent guidelines.

14 The case of cyber attack that brought down some parts of the electrical power grid of Ukraine for a substantial period of time in December 2015 is especially important, despite the existence of relatively good and secure systems locally.
Cyber-Attack Against Ukrainian Critical Infrastructure. 25.2.2016. ICS-CERT. U.S. Department of Homeland Security. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

15 IT – The New Start-Up Jobs in the Sector of Information Technologies. Program of the Government of the Republic of Serbia. Aleksandar Vučić, the Prime Minister in the Government of the Republic of Serbia. August 9, 2016. http://cdn.tf.rs/2016/08/09/EKSPOZE-1.pdf.

II PRINCIPLES AND STANDARDS ACCEPTED BY THE REPUBLIC OF SERBIA

Participation in the international scene additionally implies certain international obligations for each state towards the organisations in the work of which it takes part. In case of Serbia, the most important international obligations arise from the official strategic objective of this country to become a Member State of the European Union. In 2012, Serbia was officially granted the status of a candidate country for EU membership, and the first negotiation Chapters were opened in December 2015. The EU accession process involves harmonization of the legislative framework of the state with the existing common regulatory framework and principles of the EU. With regard to the field of information security, in the process of development of its national regulatory framework, Serbia must take into account the existing legislation in the European Union. This additionally includes the trends that are, for the time being, still in their early stages, bearing in mind that these will also most probably become common principles in the Union by the moment of Serbian accession to the EU. Umbrella EU regulations in this field primarily include the Directive concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) from 2016 and the Cybercrime Convention of the Council of Europe from 2001, as well as documents such as the Cyber Security Strategy of the European Union, A Digital Single Market Strategy for Europe, The European Agenda on Security and the like. Harmonization with umbrella regulations is obligatory for all the Member States, and it is thus also expected from states aspiring to become one. It is, however, necessary to also take into account the principles and standards prescribed in other documents mentioned here, since these can be used as guidelines in the situation in which Serbia currently finds itself in – at the very beginning of establishing of a comprehensive regulatory and operational mechanism for national information security. This is of special importance if we bear in mind the fact that the recently presented Global Strategy for the European Union's Foreign and Security Policy envisages the inclusion of cyber security issues in all policy areas, within the Common Security and Defence Policy of the Union, which Serbia is aligning with in the process of EU accession.

In regard to cooperation with NATO, Serbia, despite being a militarily neutral country that does not aspire to become its member, maintains a high level of cooperation with the Alliance, through membership in the Partnership for Peace since 2007 and through the accompanying Planning and Review Process (PARP). In January 2015, Serbia agreed the Individual Partnership Action Plan (IPAP) with NATO, thus achieving the highest level of cooperation that a country that is not a candidate for NATO membership can establish with the Alliance. Within IPAP, a partner country proposes concrete areas of cooperation that

NATO and NATO member states approve, enclosing a list of activities and envisaged time limits for their implementation. Within the aforementioned first IPAP that Serbia agreed with NATO, issues pertaining to information security are focused on the development of defence policy from cyber attacks and accompanying strategies.

Serbia must also bear in mind the coordination among international actors, such as the EU and NATO. According to the recently presented Joint statement by the President of the European Council, President of the European Commission and the Secretary General of NATO[16], the strategic NATO-EU partnership will develop over the future period beyond the existing framework, in the sense of mutual strengthening and support. One of seven co-operation measures pertains to expanding cooperation in the field of cyber security and defence, including the context of missions and operations, exercises and education and training. The European External Action Service and NATO International Staff will, together with the services of the EU Commission, develop concrete options for implementation of this concept of joint cooperation, including adequate mechanisms for coordination of staff, which will be presented in December 2016 before the Councils of both these bodies.

Obligations arising from Serbia's membership in the United Nations, as well as in the Organization for Security and Cooperation in Europe (OSCE), are mostly complied with on a voluntary basis and are predominantly based on the possibilities that developments in the field of cyber security within these international bodies provides. The possibilities are defined in the form of guidelines based on facts and practical experiences for setting up of the regulatory and operational mechanisms for raising the levels of national information security and international cooperation in this field.

EUROPEAN UNION

The Cyber Security Strategy of the European Union[17] is the first umbrella document of the European Commission in which a comprehensive strategic approach to the issue of cyber security in the EU is laid down. As its first strategic priority[18] – Achieving cyber resilience – the Strategy underlines the need for improving capabilities of the Member States and the private sector to prevent, detect and handle cyber security incidents. Issues pertaining to cyber space are mainstreamed into the external policy of the EU, within the Common Foreign and Security Policy (CFSP), which Serbia is to align with in the process of

16 Joint statement by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. 8 July 2016. NATO press release (2016) 119.

17 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013. JOIN(2013) 1 final.

18 The Strategy lays down a total of 5 priorities: Achieving cyber resilience; Drastically reducing cybercrime; Developing cyberdefence policy and capabilities; Develop the industrial and technological resources for cybersecurity; and Establish a coherent cyberspace policy for the European Union and promote core EU values.

accession to the European Union. In that sense, the Strategy additionally calls for strengthening of international efforts for the development of protection networks for critical information infrastructure through **cooperation between the states and the private sector**. Priorities set by this Strategy additionally include capacity building, international dialogue on cyber space, as well as implementation of fundamental principles of the EU, such as openness and freedom, in cyber space.

As an operational result regulating one of the areas addressed by the abovementioned Strategy, along with publishing of the Strategy, the Commission also proposed the adoption of the **Directive concerning measures for a high common level of security of network and information systems across the Union**[19] (the NIS Directive) in 2013. After three years of complicated negotiations with the European Parliament and the Council of Europe, and following significant amendments to the initial draft version drawn by the Commission, the Directive was adopted in 2016 as a binding umbrella document that should be incorporated in the national regulatory frameworks of all the Member States. The NIS Directive calls on all Member States to prescribe **the basic standards relevant to the security of network and information systems** on the national level that are to be **defined by the competent state authority and to establish a functional CERT**, along with the **adoption of a national strategy and cooperation plan** in this field.

According to the provisions of this Directive, a national strategy for information security should regulate the following issues:

- Objectives and priorities;
- Competencies and responsibilities of the relevant state bodies and other actors;
- Measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;
- An indication of the planned education, awareness-raising and training programs;
- An indication of research and development plans;
- A risk assessment plan in order to identify the potential risks;
- A list of actors involved in the implementation of the national strategy.

The Directive further prescribes that the **security measures should be based on the principle of risk assessment-based governance** – a culture that should be developed through appropriate regulatory frameworks, as well as on the basis of the existing industry practices. The **need for standardisation** is underlined as well, in order to ensure common security throughout the EU, proposing the development of harmonized standards.

19 Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. L 194/1.

The European Network and Information Security Agency (ENISA) is designated as the key body that should, in cooperation with Member States, develop guidelines pertaining to the technical areas for which standards were yet to be developed, as well as to already existing ones.

National CERTs

National CERTs, as the bodies that, among other things, have the role of hubs for information on national cyber incidents[20], are assigned a more important role through the NIS Directive in the **evaluation process of national strategies**, due to the fact that CERTs are in the position to measure the level of resilience and the general level of cyber security in different sectors on the national level, owing to the volume of information that they have at their disposal. The Member States are expected to **monitor the progress made in the area of national cyber security and to submit reports on an annual basis**. Based on these reports, the European Commission will assess the alignment of the Member States with the areas of action and objectives set in other areas as well, such as the Digital Agenda of the EU[21].

Public-Private Partnership

The NIS Directive further underlines the **necessity of cooperation between the public and the private sectors**, thus referring to establishing of mechanisms of public-private partnership. Public-private partnership is additionally underlined as an important concept in the fight against cybercrime. **The European Agenda on Security**[22] underlines the **necessity of public-private partnership** in the sense of establishing a chain for the fight against cybercrime – from the Cybercrime Centre at EUROPOL, through national CERTs, to Internet service providers that can provide warnings for the end users and technical protection. The Council of Europe's Budapest Convention on Cybercrime[23], which Serbia

20 Detailed information on the roles and tasks that CERTs most often perform based on experiences collected throughout the world is available in the report of the global Internet Governance Forum. Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security. 2014. Internet Governance Forum (IGF). https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file.

21 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. 26.8.2010. European Commission. COM(2010) 245 final/2.

22 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. The European Agenda on Security. 28.4.2015. COM(2015) 185 final.

23 Convention on Cybercrime. Council of Europe. November 23, 2001. ETS No.185.

signed in 2005 and ratified in 2009, remains the umbrella document in terms of guidelines for developing national and EU legislative frameworks in this field.

According to the NIS Directive, support to strategic cooperation among Member States is provided by the Cooperation Group that is made up of representatives of Member States, the Commission and ENISA. 18 months following the adoption of the NIS Directive, and every two years thereafter, the Group is to lay down a work program to implement the objectives set out in the Directive. **The European Union may conclude international agreements with third countries or international organisations that allow their participation in some activities of the Cooperation Group.**

Critical Infrastructure

Concerning the critical infrastructure, according to the NIS Directive the **Member States are responsible for the identification of critical infrastructure** in the field regulated by the Directive. The NIS Directive in fact recognizes two types of entities: operators of essential services and digital services providers. Annex II contains a list of services comprising the first group, based on which it can be determined whether a certain service provider can be categorized among the providers of services that are *essential* for the maintenance of critical societal and economic activities (services of special importance). According to the list of services, this group is in fact presented as equivalent to operators of critical infrastructure. Member States are obliged to, on a regular basis, and at least every two years, update the list of identified operators of essential services in their respective territories that is, together with the methodology for identification and classification of importance of the said service providers, submitted to the European Commission.

Clearer regulation of the field of critical infrastructure in the area of information and communication technologies builds upon the trend that is present in the EU since 2008 and the **Directive on the identification and designations of European critical infrastructure and the assessment of the need to improve their protection**[24], according to which the Member States are obliged to **identify the critical infrastructure on their territories** and to submit to the European Commission generic data on risks, threats and vulnerabilities, including information on potential improvements to the identified infrastructure as well as trans-border dependency. This Directive was the first to regulate the foundations for identification of critical infrastructure in the European Union and, in addition to the energy sector and the area of transport, calls on **application of the same approach in other sectors as well, specifically on information and communication technologies**. The European Commission draws up the guidelines for identification of European critical infrastructure in the Member States, but this document is classified.

24 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. 23.12.2008. Official Journal of the European Union. L 345.

In March 2009, on the basis of the **Communication on Critical Information Infrastructure Protection**[25] the **European Public-Private Partnership for Resilience** (EP3R)[26] was established **as a coordination body for a European response to cyber threats to critical information infrastructure of the Union**. The role of the Working Groups established by means of this Partnership is to, based on the model of the existing national mechanisms of public-private partnership, encourage information sharing and stock-taking of good practices; enable discussion on priorities, objectives and measures of public policies in this field; and identify the basic preconditions for security and resilience in Europe. In the meantime, in 2013, the **Critical Infrastructure Warning Information Network** (CIWIN)[27] was set up as a pilot project and a platform for exchange of information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of Critical Infrastructure Protection, with information and communication technologies included among the 11 critical sectors[28]. Despite the fact that it is primarily focused on EU Member States, the CIWIN platform also **allows access to the governmental authorities, organizations and experts from third countries** within formal cooperation with the EU on activities pertaining to the protection of critical infrastructure.[29]

As a part of the latest steps taken towards establishing an EU resilience system in cyber space, the Commission plans to conduct an assessment of risks resulting from cyber incidents in highly interdependent sectors within and across national borders, and in particular the sectors covered by the NIS Directive. On the basis of this assessment, the Commission will consider if there is a need for the development of specific rules and/or guidelines on cyber risk-preparedness for such critical sectors.[30]

25 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. "Protecting Europe for large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". 30.3.2009. COM(2009) 149 final.

26 European Public Private Partnership for Resilience (EP3R). ENISA. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

27 Critical Infrastructure Warning Information Network (CIWIN). European Commission Directorate General for Migration and Home Affairs. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm.

28 Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN). 27.10.2008. COM(2008) 676 final. 2008/0200 (CNS).

29 Membership Conditions. Critical Infrastructure Warning Information Network (CIWIN). European Commission Directorate General for Migration and Home Affairs. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/docs/ciwin_membership_conditions_en.pdf.

30 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2016) 410 final.

Standardisation

The process of standardisation is in accordance with the activities envisaged in **A Digital Single Market Strategy for Europe**[31] that has clearly recognized the importance of cyber security for functioning of the digital market. In that sense, this Strategy highlights the need to **define the missing technological standards** that are supporting the development of the digital market and services sector – **including the standards of cyber security**. The Action Plan for establishing of a Digital Single Market envisages the **adoption of a Priority ICT Standards Plan**. In addition to that, the Strategy opens the **question of establishing a Cyber security contractual Public-Private Partnership**, which was later on resolved with the adoption of the Directive on the signing of a contractual arrangement on a public-private partnership for cyber security industrial research and innovation[32].

With a view to developing a standardized approach, the **CEN-CENELEC Focus Group on Cyber Security**[33] (until 2016, the Coordination Group for Cyber Security) that is led by the European Agencies for standardisation CEN[34] and CENELEC[35], invited the European Commission to give this Group the mandate to create a framework for coordination of the **standardisation processes in the field of cyber security in Europe, as well as for the development of a regulatory framework that would allow thorough implementation thereof**.

The ENISA Governance Framework for European Standardisation[36], in addition to the **recommendations for the standardisation process**, lists the related actors that need to be included. In addition to the industry, state administration, national bodies for standardisation, the users' community and academia, the Governance Framework lists the transnational European Standardisation Organizations (ESOs) that are recognized by the European Commission, with the aim of effective exchange of knowledge and practical experiences, and thus the development of enforceable mechanisms. Among these, CEN is specifically mentioned, as an association that brings together the National Standardisation Bodies of 33 European countries.

The abovementioned **ICT Standardisation Priorities Plan** was adopted in April 2016[37] and among five priory areas, such as 5G communications and big data technologies, it includes

---

31 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. 6.5.2015. COM(2015) 192 final.

32 Commission Decision of 5.7.2016. on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. C(2016) 4400 final.

33 CEN-CENELEC Focus Group on Cybersecurity. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx.

34 European Committee for Standardisation.

35 European Committee for Electro-Technical Standardisation.

36 Governance framework for European standardisation: Aligning Policy, Industry and Research. December 2015. European Union Agency for Network and Information Security.

37 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. ICT Standardisation Priorities for the Digital Single Market. COM(2016) 176 final.

cyber security (as a separate area) among the "essential technology building blocks"[38] for establishing of a Digital Single Market. The Plan additionally envisages that, over the next three years, the European Commission will support the European Committee for Standardisation, other standardisation agencies, European regulatory bodies, as well as initiatives of public-private partnerships, including those that are focused on implementation of the NIS Directive, in the development of **standardised guidelines for risk management in the field of cyber security, as well as of accompanying guidelines for revision for supervisory authorities and regulatory bodies**.

***

Concurrently with the adoption of the umbrella legislation in this field, cyber space has been included in the foreign policy of the European Union. Namely, within the Common Foreign and Security Policy, in the **Global Strategy for the European Union's Foreign and Security Policy**[39] the issue of cyber security is defined as one of five priorities of the Union's foreign policy security issues. According to the Strategy, **weaving cyber issues across all policy areas**, as well as reinforcing the cyber elements in the Union's Common Security and Defence Policy missions and operations is envisaged. **Enhanced cyber security cooperation with partners such as the United States of America and NATO** is highlighted. In addition to that, it is stated that the EU response to cyber challenges will be **embedded in strong public-private partnership**.

Accession Negotiations of the Republic of Serbia with the European Union

Within the accession negotiations with Serbia, the European Union has so far predominantly dealt with the issues related to cybercrime, specifically in Chapter 24: Justice, Freedom and Security. **The Screening Report of the European Commission for Chapter 24** from May 2014 points to the fact that the fight against cybercrime in Serbia is in its initial phases. It was determined that Serbia had established a special unit responsible for the fight against high-tech crime within the Ministry of Interior, as well as the Special Prosecutor's Office for the fight against high-tech crime, had ratified the Council of Europe Convention on Cybercrime and that its legislation was largely harmonized with the EU Directive on attacks against information systems[40]. In addition to that, it was concluded that legislative amendments, notably those related to sanctions, were necessary to fully transpose the acquis in the part pertaining to the fight against cybercrime. It was specifically stated that Serbia had no strategy on cybercrime and that such strategy needed to be adopted. In accordance with these findings, among the measures included in the Action Plan for

38 Ibid.

39 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy. June 2016. European Union.

40 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems replacing Council Framework Decision 2005/222/JHA. 14.8.2013. L 218/8.

Chapter 24, the Serbian Government envisaged harmonization of Serbian legislation with the *acquis* in the abovementioned Directive and with the standards of the European Union in the area of the fight against cybercrime through the following activities: 1) To analyse the existing legislative framework in order to determine the level of its alignment with the *acquis* and standards of the European Union (deadline: Q1 of 2016) and 2) To prepare a draft law and bylaws on the basis of the analysis conducted (deadline: Q4 of 2016). Thus, Serbia is yet to align its legislative framework and competencies related to the issues of the fight against cybercrime.

In the recommendations issued in the Screening Report that pertain to the area of police cooperation and fight against organized crime, the Commission established the need to provide further specialized training and to enhance the capacity of the law enforcement bodies in charge of combating cyber criminality. In Serbia's Progress Reports for 2014 and 2015, the European Commission highlighted the need for strengthening of capacities of the High-Tech Crime Unit of the Ministry of Interior, with a view to achieving more efficient management of the growing range of complex criminal activity it was expected to investigate, as well as for the introduction of specialized techniques, so that this Unit was aligned with the modern operational international standards. In accordance with this recommendation, in the Action Plan for Chapter 24, the Serbian Government envisaged further provision of specialized training and enhancing of capacities of the law enforcement authorities in charge of cybercrime suppression. By means of its recommendations, the Commission additionally recognized the necessity to establish close cooperation with the private and public sectors and with the academia. In accordance with this recommendation, in the Action Plan for Chapter 24, the Serbian Government envisaged cooperation strengthening between the state authorities and civil society institutions in the area of the fight against cybercrime, through drafting and signing of a Cooperation Agreement between the state authorities and civil society institutions in the area of the fight against cybercrime (deadline: Q2 of 2016).

The issues of information security are additionally considered in Chapter 10: Information Society and Media, which comprises of three areas – electronic communications, information society services and audio-visual policy. The lead of the Negotiating Group is the Ministry of Trade, Tourism and Telecommunications. The explanatory and bilateral screenings for this Chapter were already held on May 22-23 and July 10-11, 2014, respectively, but the report and the results of the screening have not yet been made publicly available.

NATO

The Individual Partnership Action Plan (IPAP)[41] which Serbia has agreed with NATO, states enhancing capabilities for protecting critical communication and information systems against cyber attacks as future strategic goals. In this regard, the plan is to establish mechanisms and structures of coordination at governmental level for cyber defence.

The matrix of activities of Serbia's IPAP with NATO envisages the following:

1. **Development of national cyber defence policy and related strategy**, upon which to build a national cyber defence capability;

2. **Adopting necessary laws and by-laws** to identify national responsibilities and to assign required authority on cyber defence activities, harmonized with international legal norms addressing the cyberspace, including the Council of Europe Convention on Cyber Crime;

3. **Establishment of government-level mechanisms and cyber defence structure for coordination of and conducting cyber defence activities**;

4. **Complete the implementation of a fully mandated operational Computer Security Incident Response Capability (CSIRC)**, that can prevent, monitor, detect, defend against and recover from cyber attacks against government civil and military critical communication and information infrastructure;

5. **Establish international coordinating mechanisms** that enable real-time interaction with other states and international organizations **to respond effectively to cyber attacks and to allow information exchange**.[42]

Defending against cyber attacks is also referenced in Chapter 4, Protection of Classified Information, within Goal 3: Enhance capabilities for protecting critical communication and information systems against cyber attacks. The description of activities for fulfilment of this goal refers to the mentioned chapter 1.2.3.[43]

Therefore, Serbia should legally define the legislative framework and competence for matters of national defence against cyber attacks. Although, IPAP is a document developed and implemented virtually on a voluntary basis, i.e. it is not formally and legally binding and there are no specific sanctions if any of the envisaged activities are not fulfilled, the

41 Chapter 1.2.3. Current Security Challenges: The fight against terrorism, arms control and defence against cyber attacks. Individual Partnership Action Plan (IPAP) of the Republic of Serbia and the North Atlantic Treaty Organization. December 2014. Ministry of Foreign Affairs of the Republic of Serbia.

42 Chapter 1.2.3. Current Security Challenges: The fight against terrorism, arms control and defence against cyber attacks. Individual Partnership Action Plan (IPAP) of the Republic of Serbia and the North Atlantic Treaty Organisation. December 2014. Ministry of Foreign Affairs of the Republic of Serbia.

43 Ibid.

mere fact that the activities, i.e. areas of cooperation are proposed by the partner state indicates that there is a will to implement them. The contrary would create an impression of a lack of responsibility and/or basic understanding of activities that the partner state chose itself independently.

ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE)

As part of the activities focused on security and other issues such as arms control, measures to build security and confidence, human rights, and similar issues, the Organization for Security and Cooperation in Europe (OSCE) also deals with the issues of cyber security in the form of fight against terrorism and cybercrime. In this regard, in 2013 the Member States adopted the first package of Confidence Building Measures (CBMs) to reduce the risk of conflict caused by the use of information and communication technologies. The 11-measure package, among other things, includes the exchange of information on cyber threats; safety and use of ICT systems; national organizations, strategies and terminology; holding consultations in order to reduce the risk of misperception and possible emergence of tension; exchange of information on measures taken to ensure an open and secure Internet; nomination of national contact points; and the role of the OSCE as a platform for dialogue.[44]

The second set of measures, adopted in March 2016, builds upon the previous guidelines, adding five new ones. Besides better defined principles of data exchange, the new guidelines directly urge the Member States to promote and improve mechanisms of public-private partnership aimed at a common response to threats. In addition, the penultimate guideline (No. 15) refers to the critical information infrastructure upon which the functioning of critical infrastructure depends, providing several models of cooperation in this area.[45]

Although adoption and implementation of the proposed measures is based on the principle of voluntarism in each state, they serve as specific guidelines for institutionalization of a regular dialogue between the states at various levels, with a clear incentive for the development of principles of public-private partnership.

In the meantime, the decision of the 18th session of the OSCE Ministerial Council, which came into force in February 2012, appointed Serbia as the Chair of the OSCE in 2015, as part of its joint candidacy with Switzerland, which chaired in 2014. As part of the program

---

44 Decision No.1106. Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 3.12.2013. Organization for Security and Cooperation in Europe. PC.DEC/1106.

45 Decision No.1202. OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 10.3.2016. Organization for Security and Cooperation in Europe. PC.DEC/1202.

for the chairmanship period 2014-2015, permanent representatives of Switzerland and Serbia presented the Joint Work plan, specifying in Chapter 3, Transnational threats and challenges, the strengthening and further development of the OSCE contribution in the area of information/cyber security as one of the measures.[46] As part of the commitments in this area, during its OSCE Chairmanship Serbia organized a two-day conference on efficient strategies for cyber/ICT security threats.[47]

UNITED NATIONS

In response to the initiative of certain Member States, the United Nations General Assembly mandated the Secretary General to establish a Group of Governmental Experts (GGE) for activities in the area of information and telecommunication technologies in the context of international security. The first Group, which began its activities in 2004, failed to reach consensus and a joint report, mainly because of disagreements over the impact of ICT on national security and military issues, as well as over the framework of the Group's operation (i.e. whether it should deal exclusively with matters of ICT infrastructure or the content as well). The second Group, established in 2009, had more success – it published a joint report the following year[48] with several recommendations directed at strengthening the dialogue, cooperation and exchange of information among countries, as well as at capacity building.

The turning point was the third Group's report from 2013[49], which confirmed that existing international law applies to cyberspace, but also the sovereignty of States over the ICT infrastructure on their territory, as well as the need to balance between information security and respect of human rights and fundamental freedoms. The 15 members of the Group comprised of experts from leading world powers, including the United States, Russia, China, Great Britain, India, France, Germany, Indonesia and Japan.

46 Joint Work plan of Switzerland and Serbia. 28.6.2013. Organization for Security and Cooperation in Europe. PC.DEL/600/13.

47 OSCE workshop in Belgrade highlights need for cyber strategies and effective co-operation mechanisms to reduce risks of conflict using ICTs. 30.10.2015. Organization for Security and Cooperation in Europe. http://www.osce.org/cio/195986

48 Report of the Group of Governmental Experts on Developments in the Area of Information and Telecommunications in the Context of International Security. 30 July 2010. United Nations General Assembly. UN DOC A/65/201.

49 Report of the Group of Governmental Experts on Developments in the Area of Information and Telecommunications in the Context of International Security. 24 June 2013. United Nations General Assembly. UN DOC A/68/98*.

The fourth Group's report from 2015[50] made a step further, confirming the responsibilities of states in respect of the principle of state sovereignty when using its own ICT systems, amicable dispute resolution in cyberspace, refraining from intervention in the internal affairs of other states with respect to the use of ICT, as well as protection of human rights and fundamental freedoms on the Internet. The report, later adopted at the General Assembly, has also brought a series of measures, implementation of which is voluntary, including the one that countries will not intentionally damage another's critical infrastructure or CERTs through cyber-attacks, and that they will mutually assist each other in investigating cyber attacks and in cases of cybercrime originating from their territories. 20 countries took part in the work of the fourth Group, including those from 2013.

The work of the GGE from its first report in 2010 until today has positioned it as the key international mechanism for discussion - and quite possibly for reaching agreement – on standards and actions for confidence-building in cyber space that states should seriously take into consideration. The fifth Group was initiated by the decision of the General Assembly in December 2015[51] and formed in early 2016. Its report, should an agreement be reached, is expected in 2017. By the decision of the UN Secretary-General, in accordance with the nomination of the Ministry of Foreign Affairs, Serbia has its representative in this Group coming from the ranks of the Ministry of Defence, which on one hand allows for the participation of the state in making decisions and creating recommendations and standards in the area of cyber-security at the international level, while on the other hand it brings the potential of having this issue receive more attention in the forthcoming period, especially in terms of implementation of adopted measures and adoption of best international practices at the national level.

50 Report of the Group of Governmental Experts on Developments in the Area of Information and Telecommunications in the Context of International Security. 22 July 2015. United Nations General Assembly. UN DOC A/70/174,

51 Developments in the area of information and telecommunications in the context of international security. 30 December 2015. United Nations General Assembly. UN DOC A/RES/70/237.

III LAW ON INFORMATION SECURITY

The Law on Information Security[52] adopted by Serbia on January 26, 2016 is the first umbrella law regulating protective measures against security risks in information and communication systems, the liability of legal entities in the management and use of information and communication systems, and defining competent authorities for implementation of protective measures.

One of the most important legal novelties is the establishment of the National Centre for Prevention of Security Risks, which according to international practice is the Computer Emergency Response Team (CERT), the body responsible for quick response in case of incidents, as well as for collection and exchange of information on security risks for information and communication systems. The national CERT is under the competence of the Regulatory Agency for Electronic Communications and Postal Services (RATEL). The establishment of a national CERT is at the same time one of the basic obligations prescribed by the EU NIS Directive, also the obligation of all Member States, as well as a step that all candidate countries should have in mind.

The Law also regulates issues such as ICT systems of special importance and measures for their protection (which is also one of the requirements in accordance with the NIS Directive) and provides basic regulation for the area of crypto-security and protection against Compromising Electromagnetic Emanations (CEE). It envisions the formation of information security inspections, to supervise the implementation of Law and the work of operators of ICT systems of special importance, which is the responsibility of the Ministry responsible for information security affairs, currently the Ministry of Trade, Tourism and Telecommunications.

Finally, the Law envisions the establishment of the Body for the Coordination of Information Security as a coordinating body for realization of cooperation and harmonized performance of activities aimed at improving information security, as well as initiation and monitoring of preventive and other activities in the area of information security. The Coordination Body - which was established by the Decision on Establishment of the Body for the Coordination of Information Security on March 8, 2016 - although mainly an advisory participant pursuant to the Law, potentially opens up opportunities for a more comprehensive approach to information security by providing for the formation of expert working groups which may include representatives of other public authorities, industry, the academic community and

52 Law on Information Security. "Official Gazette of the RS", No. 6/2016.

civil society. That way the Coordination Body presents an indication of political will (or at least the lack of resistance) towards formation of public-private partnerships in specific areas of information security, which is not often the case in Serbia, especially to leave potential space for something like that within the respective law itself.

However, despite the unquestionable necessity of having a Law that regulates the field of information security, some areas in the document that is currently in effect remain under-regulated, which leaves space for individual interpretation, but may also pose as a potential security risk.

Although referring to the principle of risk management, the Law does not explicitly prescribe risk assessment and analysis, or defining a methodology based upon which these would be carried out, as an initial obligation for any subsequent activity - from the selection of adequate protection measures, through the Act on Security of ICT Systems to be developed and adopted by their operators, to the definition of the role of the national CERT and CERT of republic authorities that should provide early warnings on the risks and perform security risk prevention activities. Without adequate risk assessment at an early stage it remains unclear what risks need to be overcome, and what can be tolerated, which in itself carries a security risk of wrong allocation of adequate resources for incident prevention and resolution. Comprehensive risk assessment and analysis in the area of information security could therefore be one of the initial activities envisaged by the pending Strategy for the Development of Information Security in order to overcome this omission.

With respect to incident response, the Law largely leaves notification and coordination to the competent authority, i.e. the Ministry in charge of information security (in the new term of the Government this is again the Ministry of Trade, Tourism and Telecommunications), instead to the newly established National CERT, which unnecessary bureaucratizes the operational mechanism and puts additional strain on an already overburdened Ministry. Also, there is the prescribed principle of "guild" notification on incidents (through the National Bank of Serbia, RATEL and other specific bodies), which undermines the essence of the national CERT's existence as a single operational and communication point of confidence with regard to incidents. Finally, although the national CERT is placed within RATEL as the existing institution, there is neither an envisaged deadline for its establishment nor are there mechanisms to provide the necessary resources for efficient operation of this new operating body[53].

The Law has also envisaged the adoption of bylaws, proposed by the competent ministries. By adopting adequate and detailed bylaws, guided by mentioned obligations, but also by examples of good practice, it is also possible to overcome some of the perceived shortcomings

53 Having in mind that the CERT shall employ proven experts in the area of information technologies, their salaries must be in the range of salaries offered by the private sector for the same expert profile, in order to maintain quality staff and to avoid hiring unqualified staff. Also, given the dynamics of development in this field (threats and response mechanisms), as well as the necessity of regular contact and cooperation with international CERTs and professional organizations, permanent resources for training and participation in international conferences are required, as well as new software and hardware solutions, and even for additional people.

in the existing Law. It is imperative, however, that the bylaws are passed in close cooperation with private and non-governmental sectors, as well as professional and academic communities, to ensure that they do not repeat some of the mistakes that were made in the very Law, and allow for meaningful implementation of the proposed solutions.

When it comes to the prescribed legal obligations, particular attention needs to be paid to clearly define the contents of the Act on Security of ICT Systems of special importance, as well as the internal audit procedures of ICT systems of special importance. This should be kept in mind when developing the Decree foreseen by the Law, which deals with these issues. In order to have a high level of security, the Act on Security of ICT Systems needs to be based on an adequate risk assessment and analysis for the reasons mentioned above, particularly bearing in mind that these are systems of special importance. Having in mind the extreme dynamics of development in the area of information technology, the Decree should also define the mandatory revision of the act every 12 months, as well as in case of an incident. When it comes to internal audits of ICT systems, certain external audits should also be prescribed. These audits could be performed by the National CERT or special registered CERTs, for a fee. This could ensure the economic viability of CERTs, as well as a mechanism for higher levels of information security contributing to the development of the national economy. The same solution could be applied to the position of the security inspector, as defined by the Law, in case it turns out that the competent Ministry does not have adequate capacities for this activity or in case of complications and delays caused by amendments to the systematization of positions at the Ministry in order to create these.

Likewise, in order to harmonize the Law on Information Security with the existing regulatory framework in Serbia, the solutions it provides need to be harmonized with other existing laws, or the competences between them need to be clearly separated by possible bylaws. This is particularly important, for example, when it comes to the Data Secrecy Law[54]. Current solutions in the Law on Information Security do not make a precise distinction between secret, personal and sensitive data, which is why its provisions often reference the Data Secrecy Law.

This framework leaves room to solve a specific incident both in accordance with one and the other law, i.e. it leaves a situation where the competences of the two laws overlap, which further leaves room for interpretation and possible defaults. Other than this, the Law on Information Security has not explicitly defined who the national authority for crypto-protection is. Namely, Articles 20-25 of the Law on Information Security determine that the Ministry of Defence is competent for this issue, but do not specify which organizational unit exactly, and the Law does not envisage adoption of a specific bylaw to regulate this matter more closely.

Finally, the functioning of the Coordination Body, especially the way envisaged expert work groups are formed, can be more clearly defined through the envisaged Rules of Procedure of this body. Bearing in mind the fact that the position of the Coordination Body is not defined in sufficient detail by the adopted Law, possible amendments and addenda thereof

54 Data Secrecy Law. "Official Gazette of the RS", No. 104/2009.

can already be considered, to allow more efficient functioning of the Body in accordance with a clear framework. This would include the sectors of public administration that have been mistakenly omitted from participation in the Body, and above all the Ministries responsible for the economy, transport, education and science, technological development and information, as well as bodies such as RATEL, RNIDS and the Commissioner for Data Protection. Also, this would allow easier development of cooperation with other actors in the future within the aforementioned concept of public-private partnership in the area of information security, all with the aim of a more comprehensive approach to this issue. In the future, this would establish direct cooperation and confidence among actors and sectors, and set the basis for a multipartner model for designing policies on cyber security, which would bring direct benefit both to the state and other sectors.

However, taking into account the level of regulatory development globally present in the area of information security, as well as growing challenges that daily use of information and communication technologies bears, the fact that Serbia adopted the Law on Information Security is of utmost importance, which provides some initial points for constructive solutions. Considering the speed of development of opportunities but also challenges and risks in this field, it is necessary to continuously follow global trends and good practice. In terms of this, some of the shortcomings in the Law can be overcome in the short term with detailed solutions provided in the bylaws to be adopted by the Government, modelled on successful solutions found in the existing international practice. Additional solutions can also be incorporated in the expected Strategy for the Development of Information Security and the accompanying Action Plan. In the long term, however, it is anticipated that the "lifetime" of this Law is limited to a maximum of two years, when the deadline for full compliance with the NIS Directive will expire.

IV INFORMATION SECURITY STRATEGY: BASIC ELEMENTS AND GUIDELINES

A clearly defined strategy in any area enables government authorities to translate political vision into coherent policies that can be implemented. It is therefore imperative for an information security strategy to clearly define the basic terms it regulates, starting with the vision, mission and goals as basic indicators of the direction in which the state plans to develop this area, both for national actors and international partners.

In developing the strategy, it is necessary to have a clear perception of the initial state of affairs it deals with and further develops and improves. Therefore, risk assessment and analysis is a necessary precondition for a strategy that addresses key issues, providing specific solutions for observed weaknesses and anticipating real, enforceable actions to improve the current situation.

The further lifecycle of the strategy involves a comprehensive, inclusive approach that involves all relevant actors, starting from those who decide on it, to those who monitor its implementation and in particular those to which it relates. Substantial involvement of all relevant actors at an early stage of the document's development provides greater agreement and support, and thus creates conditions for selection of realistic, enforceable activities through a joint effort. This approach implies involvement of the private sector, whereby the strategy itself becomes a product of constructive public-private cooperation, allowing for more efficient communication and optimization of planned future activities, and timely exchange of information and sharing of resources. The latter can be extremely useful primarily to technologically underdeveloped administrations.

Upon expiration of one cycle of strategy implementation, the last necessary step requires analysis and evaluation of the implementation process and final results. This step will allow designing the succeeding strategy as an even more focused document, based on the perceived successes, as well as shortcomings and/or mistakes in the previous cycle.

In this sense, guides and guidelines for the development of national cyber security strategies serve to support this process, especially in the elements and activities on which there is already a standardized mutual agreement among international bodies and organizations that these present as an indispensable ingredient of quality cyber security strategies.

The ITU National Cyber security Strategy Guide[55], for example, contains a draft of the initial design of a national strategy for cyber security, as well as a list of technical solutions that may be applied to achieve the most common security goals, which can be useful in creating a national strategy as well as the accompanying action plan.

RISK ASSESSMENT

The European Cyber Security Strategy stresses the importance of establishing fact-based risk assessment and developing a culture of risk management in security cyber communities of the EU. Accordingly, the Practical Guide on Development and Execution of national cyber security strategies[56] developed by ENISA underlines the need for performing comprehensive risk assessment in order to determine the goals and scope of the strategy. Risk assessment consists of three steps: identification, analysis and risk assessment.

Risk assessment and analysis provide insight into the initial state of affairs the strategy is dealing with and aims to develop, thus being the necessary precondition for forecasting real, enforceable activities. This step allows harmonization of the strategy's goals with national security goals, but also ensures that the focus of the strategy is on the most important challenges when it comes to cyber security. Without adequate risk assessment at an early stage it remains unclear what risks need to be overcome, and what can be tolerated on the road to fulfilling the goals of the strategy. The risk then becomes greater due to the fact that, for example, there is a possibility that some critical network/systems are left insufficiently protected. On the other hand, it opens the possibility that resources are used inefficiently if imposed protection mechanisms are higher than necessary when it comes to risks that can be tolerated.

Similarly, the National Cybersecurity Framework Manual[57] states the practice of early identification of critical services to society, i.e. critical information infrastructure in the process of risk assessment. This practice helps to formulate a quick response to potential incidents that threaten the security of information and communication systems of special importance.

Microsoft has also noted the necessity to identify existing risks and incidents in the process of developing the document, and then to establish a standardized method of response to such and similar incidents as a permanent framework. As a basic step for the establishment of such a mechanism, the strategy must clearly define what constitutes cyber

55 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

56 National Cybersecurity Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

57 A. Klimburg (Ed.). National Cybersecurity Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

incidents at the national level that require state involvement and activation of protection plans and procedures for response to incidents[58]

FORMULATION OF GOALS

National strategies typically define certain groups of standard, (more) general goals, as does, for example, the European Cyber Security Strategy: achieving cyber resistance (development of capabilities and efficient cooperation with private sector and the general public), protecting critical information infrastructure, reducing cybercrime, developing industrial and technological resources for cyber security and contributing to the creation of international policy on cyber space, while preserving a free and open cyber space.

Clearly defined goals within the strategy provide guidelines to decision makers and other relevant actors on political priorities in the area of cyber security, as well as on potential resource allocation[59] At the same time, clearly defined goals refer to activities, and thus enable clear division of roles and responsibilities among relevant actors, creating conditions for the development of mechanisms for potential optimization through the division of activities and resources. Finally, clearly defined goals also help develop trust in the international arena, pointing to the strategic direction in which a specific state is developing in the given field, making it a predictable actor.

For ease of monitoring and analysis of progress in implementing national cyber security strategies and the achievement of defined goals, ENISA proposes to also define key performance indicators (KPIs)[60] These indicators actually present a list of activities and results to be fulfilled on the basis of specific goals defined by the strategy. In this regard, developing key performance indicators can serve as a direct preparation for designing an action plan to implement the strategy, but also for the process of evaluation after the envisaged deadline for implementation of the strategy expires, as well as for periodic reports on this topic.

58 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

59 A. Klimburg (Ed.). National Cybersecurity Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

60 An evaluation Framework for National Cybersecurity Strategies. November 2014. European Union Agency for Network and Information Society.

CLEAR DIVISION OF COMPETENCES AND RESPONSIBILITIES

In order to ensure effective implementation of the strategy, ENISA's Practical Guide on Development and Execution of national cyber security strategies[61] emphasizes the need to define a clear governance structure, by unambiguously defining the roles and responsibilities of key actors. This ensures coordination of various activities envisaged by the strategy and at the same time provides control over its implementation. This way the body responsible for coordinating the strategy is able to consider all the advantages and disadvantages of the strategy in the process of audit and evaluation, to summarize results and lessons learned and to propose effective measures for the next cycle of development of the national strategy.

As a prerequisite for this step, it is also necessary to have a clear picture of all relevant actors and their competences, activities as well as capacities, as defined by other existing laws and regulations. In this way, the strategy takes into account the existing regulatory and technical framework and is compatible with them, which in turn facilitates its implementation.

The *National Cybersecurity Strategy Guide*[62] of the International Telecommunications Union (ITU) specifically proposes a cyber security management structure, where the main bearer of responsibility would be the government of the state itself, while the role of a national coordinator for cyber security would be on the specific, relevant ministry or a special body established for this purpose. The competent ministry would be responsible to direct and coordinate policies related to cyber security, respond to incidents, advocate the development of a culture of cyber security in the form of campaigns or special education programs and develop capacities and basic standards. As a formal framework for monitoring, warning and responding to incidents, the ITU states the creation of CIRTs, which is now, by the adoption of the NIS Directive, binding on EU Member States and something that candidate countries must also have in mind.

COMPREHENSIVE INCLUSIVE APPROACH

A comprehensive, inclusive approach, involving all relevant actors at an early stage of strategy development also provides greater agreement and support of actors to which it applies and thus creates conditions for selection of realistic, enforceable activities. This

61 National Cybersecurity Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

62 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

approach also implies involvement of both the private and civil sectors, thereby making the strategy itself become the product of constructive public-private cooperation, enabling more efficient communication and optimization of planned future activities, i.e. timely exchange of information and allocation of resources, which can be extremely beneficial, especially for technologically underdeveloped administrations.

In order to establish a comprehensive mechanism for cyber security, the ITU's National Cyber Security Strategy Guide[63] emphasizes the necessity of establishing a public-private partnership at all levels. The basic principles that should underlie this kind of public-private partnership are: exchange of information on policy development among all related actors; exchange of knowledge and experience through joint training programs in order to compensate for deficiencies in the educated workforce in this area; real-time exchange of information on cyber threats and vulnerabilities, which is supported by the work of CERTs in the comprehensive monitoring of the national cyberspace. The ITU defines three preconditions for successful public-private partnership:

- Understanding mutual benefits from partnership, bearing in mind expert information, knowledge and support that the private sector could offer to the state, while the state plays a key role in creating a regulatory framework favourable for further functioning and development of the private sector;

- A clear division of roles and responsibilities where the state has key responsibility and resources for coordination of activities in cyberspace, while the private sector has the expertise and resources to improve the processes and mechanisms for higher levels of cyber security;

- Development of trust.

STANDARDISATION

In order to harmonize different approaches to cyber security in both the public and private sector, enable effective exchange of information, as well as achieve optimization in terms of prioritization of investments in the cyber security field, the strategy should prescribe and define the sector's minimum (basic) security standards. ENISA recommends these standards to be defined through a process of public-private partnership taking into account good security practices and existing standards and mechanisms, but also the practice that is far more developed by the industry. Once standards are established, it is necessary to define the responsible person and/or body to monitor application of these standards. The

63 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

application of defined standards can be encouraged by the development of a model for self-assessment (*security maturity self-assessment tools*)[64]

In the process of creating bylaws it is necessary for the Decree envisaged by Article 8 of the Law on Information Security, related to the adoption of the Act on Security of ICT Systems, to clearly define minimum security mechanisms that ICT system operators must adopt, especially considering that these are ICT systems of special importance.

Likewise, it is necessary to clearly prescribe the criteria for definition of incidents in terms of type and importance in order to ensure greater security and more efficient exchange of information, but also response to the very incidents when they occur. In this regard, the EU Directive on attacks against information systems[65], which prescribes the basic rules with respect to the definition of criminal offenses and sanctions in the area of attacks on information systems may be used as one of the guidelines for defining more closely the incidents within the Decree on the procedure for submission of data, lists, types and character of incidents and the procedure of informing the competent authority on incidents in the ICT systems of special importance, which is drafted, as Article 11 of the Law on Information Security prescribes, by the Ministry of Trade, Tourism and Telecommunications.

ENISA mapped several key actors involved in the exchange of information. In the first place these are CERTs, which have access to different levels of data, such as data about vulnerabilities, malware infections and developments and cyber incidents. These data can serve as elements for development of the above mentioned key performance indicators based on which efficiency of the solutions envisaged by the strategy of cyber security and those implemented, i.e. the actions taken, are monitored. National regulatory bodies, which mainly have a role of a hub for information on national cyber incidents, are the second key actor for the exchange of information[66] This approach is also defined by the NIS Directive, primarily for sectors of special interest.

Communication between CERTs enables greater operational cyber security in the technical sense, but also the development of confidence between actors, which is particularly important when it comes to cooperation between public and private CERTs. Regular exchange of information on one hand enables optimization through the exchange of capacities that are known to all parties in the process, while at the same time, timely exchange of information enables efficient response in case of incidents.

Efficient information sharing also contributes to increasing awareness on the need for cyber security among all relevant actors. In practice, there is a noticeable trend whereby the main challenge is how to stimulate the middle management at institutions and

---

64 National Cybersecurity Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

65 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. 14.8.2013. Official Journal of the European Union. L 2018.

66 An evaluation Framework for National Cybersecurity Strategies. November 2014. European Union Agency for Network and Information Society.

organizations to coordinate their activities with the prescribed principles and standards in order to implement adopted strategies and action plans. One of the suggested mechanisms to overcome this obstacle is the creation of a cross-sector coordinating group of middle management for more efficient harmonization of various requirements of government authorities and a better understanding of decision-makers when it comes to technical requirements, which come from the professional community and customers, translating these into policy language.[67]

OPTIMISATION: EXCHANGE OF CAPACITIES

Microsoft, as a company that is actively involved in the establishment of mechanisms for cyber security and the definition of minimum security standards, both for national cyber security strategies[68], and cyber strategies of cities and local self-governments[69], has emphasized the possibility of establishing a model for alerting of threats and weaknesses in relation to the most significant cyber threats at the national level and creating a framework for acting based on this information. Considering that the efficiency of such mechanism depends on the exchange of information and timely response to it, Microsoft has emphasized the necessity of public-private cooperation in order to optimize and respond faster.[70]

In the event of a national cyber incident, the private sector may play an important role in the response and overcoming the consequences of it. In the process of digitalisation of state administration, for example, the private sector may significantly contribute with its knowledge, experience and established standards in the development of mechanisms for defence against cyber incidents.

This is why it is necessary to envisage, but also facilitate cooperation between the public and private sectors if an incident occurs. Apart from a normative framework that would envisage this, the industry proposal is to conduct joint exercises of response to incidents in which both sides would participate in order to establish clear procedures for response, the chain of command and responsibilities of both sides.[71]

---

67 A. Klimburg (Ed.). National Cybersecurity Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

68 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

69 Flynn Goodwin, C. and Nicholas, J. P. 2014. Developing a City Strategy for Cybersecurity. A seven-step guide for local governments. Microsoft Corporation.

70 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

71 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

EDUCATION

The Cyber Security Strategy of the European Union has envisaged the following national programmes for education and training in the area of network and information security: training on network and information security at schools, training on network and information security and development of security software, as well as protection of personal information for students of information technology and computer science and basic training for employees at the state administration.[72]

ENISA recommendations for national cyber security strategies include consideration of the development of national training programs on information security, as well as separate modules at universities that would not deal solely with the technical aspect of cyber security. Instead, they would offer a more comprehensive approach to this area. In order to develop education programs ENISA recommends the creation of a catalogue that would map the labour market in the area of information security and formulate programs in accordance with the perceived shortages of available skilled staff.[73]

Development of technical and political capacities of institutions and organizations is also one of the priorities of almost all international forums, as well as the European Union itself. Due to the complexity of the area and the fact that no one can defend against cyber attacks independently, capacity building requires a multidisciplinary approach and cooperation between the public, private and civil sectors. This can be done through investment in specific programs for capacity building in Serbia, as well as through systematic use of existing global programs of international bodies and organizations such as the Council of Europe, ENISA and the ITU, forums, such as the Internet Governance Forum or the Global Forum on Cyber Expertise, companies such as Microsoft, professional communities such as the FIRST community of CERTs and independent and educational institutions such as DiploFoundation, the Geneva Centre for Security Policy and DCAF.

EVALUATION

Evaluation is a necessary final step in the life cycle of the strategy, which must be clearly envisaged in the document itself in order to be binding. Evaluation provides insight into the efficiency and effectiveness of implementation of the strategy and the accompanying action plan, but also into the extent to which the planned measures were realistic or not. The evaluation process enables defining future goals and allows amending the strategy

72 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013. JOIN(2013) 1 final.

73 National Cybersecurity Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

depending on the needs and circumstances, in accordance with perceived successes, shortcomings and/or mistakes from the previous cycle.

ENISA advises to have external evaluation, after conducting a self-evaluation, and to include relevant and related actors. Each separate activity should be evaluated on the basis of developed, specific and measurable key performance indicators.[74]

In the context of a fact based approach - that ENISA supports - evaluation and strategic programming is one of the fundamental principles on which a cyber security strategy is based, with the inclusion of all relevant institutions. This approach has already been implemented in the European Union through the concept of the European Digital Agenda, as well as in the recently adopted NIS Directive, as a starting element for a cyber security strategy that links this field with the wider goals of promoting an inclusive and safe digital society and enabling economic growth. Member States are expected to follow the progress of national cyber security and report annually. Based on these reports, the European Commission will assess the compliance of Member States with the areas of action and goals set out within the plans defined by the Digital Agenda.[75]

NATO stresses the need of having mechanisms for revision and assessment of strategies, arguing that if these mechanisms are left out, the process of creating a strategy risks to become a one-time exercise that depends on political will.[76]

The industry applies the same practice, and in this sense Microsoft, for example, is guided by the principle that the dynamic nature of cyber security conditions risk management based on the regular update of strategic responses to threats and challenges, and that a national strategy should include an audit process within its key principles.[77]

74 National Cybersecurity Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

75 An evaluation Framework for National Cybersecurity Strategies. November 2014. European Union Agency for Network and Information Society.

76 A. Klimburg (Ed.). National Cybersecurity Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

77 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

V POSSIBILITIES

Participation in the international arena brings, apart from international obligations, certain opportunities for every state. In this sense, Serbia, as a candidate country for membership in the European Union, has access to certain EU funds, such as Horizon 2020, the fund for research and innovation, and the Instrument for Pre-Accession Assistance (IPA II instrument). In addition to this, the European Union provides the possibility to use resources from other instruments and programs through which the beneficiary country can obtain support for the development of information security in terms of development of CERTs and national information security strategies, as well as raising awareness in society on this issue.

In addition, Serbia has access to the resources provided by NATO's *Science for Peace and Security program*, and the ability to use the support of the Alliance through the establishment of specific goals of cooperation within the framework of Individual Partnership Action Plans, which are agreed on a two–year basis. Apart from this, Serbia has access to programs under NATO's *Smart Defence concept*, focused on the field of cyber defence.

Also, Serbia is a member of the International Telecommunications Union (ITU), which, in cooperation with the International Multilateral Partnership Against Cyber Threats (IMPACT) provides support to ITU member states for activities such as implementation of national risk assessment and analysis in the area of information security, development of national information security strategies and establishment of national CERTs.

EUROPEAN UNION

Horizon 2020 is certainly the most important fund of the European Union, which promotes research and innovation[78]. This program is the successor of the EU's Seventh Framework Programme for Research (FP7), which funded research projects in the period 2007-2013. Horizon 2020, being implemented in the period 2014-2020, has a much wider scope (encouraging and funding research and innovation) compared to FP7, a bigger budget, simplified procedures for participation, and openness to new actors/potential beneficiaries (e.g.

78 Horizon 2020: The EU Framework Programme for Research and Innovation. European Commission. https://ec.europa.eu/programmes/horizon2020/.

small and medium-sized enterprises are included). In addition, this program has incorporated two more EU programs alongside FP7[79].

The work program of Horizon 2020 for the period 2016-2017 envisages funding of research in three areas: *Excellent Science, Industrial Leadership* and *Social Challenges*, with a total value of 16 billion Euros[80]. Calls for projects related to cyber security are grouped largely within the area of *Social Challenges*, sub-section *Secure Societies – Protecting freedom and security of Europe and its citizens*. From a total of five calls for projects under this sub-section, two are relevant to cyber security: *Protection of critical infrastructure* (dealing with topics that connect the physical and cyber security of critical infrastructure), and *Digital security* (cyber security for small and medium-sized enterprises, local administrations and individuals; the economy of cyber security; cooperation at the EU level and international dialogue on research and innovation in the area of cyber security and privacy; cryptography; issues of advanced threats in cyber security and actors of these threats, privacy, data protection, digital identities)[81].

Serbia joined the Horizon 2020 program on July 1, 2014. The Ministry of Science, Education and Technological Development is responsible to provide support to all program blocks and topics of Horizon 2020 through the established network of National Contact Points[82]. In addition, Serbia established an expert working group "Horizon 2020", and set up the Centre for the Promotion of Science as an institution that will deal with the promotion of this important program. In this regard, the Centre organizes the program *Horizon on Thursdays*, which promotes this program every Thursday to the interested professional public and citizens. On February 11, 2015 the program *Horizon on Thursdays* focused on IC technology[83]. One of the key preconditions for participation in such projects is formation of a consortium of institutions throughout the territory of Europe, most often made up of mixed actors - from the government, private, civil and academic sectors. While this brings a certain complexity in terms of preparation and implementation of the project, it also brings direct benefits in the form of exchange of experiences among countries and actors and strengthening cooperation.

Another fund within which Serbia can develop capacities in the area of cyber security is the **Instrument for Pre-Accession Assistance 2014 - 2020 (IPA II instrument)**, which annually allocates around 200 million Euros for Serbia. IPA II takes up a sectorial approach in planning activities during the implementation period. It is directed at a smaller number of strategic sectors identified by IPA II beneficiary countries and the EU institutions and defined in the Sector Planning Document (SPD) for the country. One of the sectors includes

79 Innovating aspects of the program Competitiveness and Innovation Framework Programme (CIP) and the EU contribution to the European Institute of Innovation and Technology.

80 Horizon 2020: new Work Programme supports Europe's growth, jobs and competitiveness. Fact sheet. 13.10.2015. European Commission. http://europa.eu/rapid/press-release_MEMO-15-5832_en.htm

81 A guide to ICT-related activities in WP2016-17. European Commission. https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/Guide%20to%20ICT-related%20activities%20in%20WP2016-17%20A4%20v8.pdf.

82 Horizon 2020. Framework program of the European Union. http://horizont2020.rs/

83 H2020 and ICT. Centre for the Promotion of Science. http://www.cpn.rs/aktivnosti/h202-i-ict-2/

internal affairs and, within these, the fight against cybercrime. Activities envisaged in this area are to be implemented in the period 2018-2020[84].

As part of this instrument, there is an additional EU fund, the so-called Multi-Country IPA. The aim of this fund is to strengthen regional cooperation in certain sectors, enable participation of each country in the region, but also to reduce total costs as a result of its scope and focused goals. One of the priorities of this EU program is the fight against organized crime and, as part of this priority, the fight against cybercrime. Here the EU relied on capacities of the Council of Europe, which implemented the project CyberCrime@IPA[85] in the period 2010-2013 in the Western Balkans, and is currently implementing the iPROCEEDS project (2016-2019)[86], both funded through the aforementioned Multi-Country IPA. The full name of the CyberCrime@IPA project is "Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime", and the beneficiaries of this program were Albania, Bosnia and Herzegovina, Croatia, Montenegro, Macedonia, Serbia, Turkey and Kosovo*. The goal of the project was to strengthen the capacity of the judicial authorities in criminal law to effectively cooperate against cybercrime on the basis of the Budapest Convention on Cybercrime and other standards and tools[87]. Overall, progress has been made on all the recommendations, but above all in raising awareness, strengthening cooperation between the public and private sectors in this field, as well as in strengthening regional and international cooperation in the fight against cybercrime.[88] The IPROCEEDS project aims to strengthen the capacity of government authorities in the IPA region to seek, seize and confiscate revenues generated through cybercrime and to prevent money laundering on the Internet.

Within the framework of its **Instrument contributing to Stability and Peace** (IcSP)[89], the European Commission funds EU actions in the area of foreign policy, primarily aimed at conflict prevention, peace-building and preparation for crisis response in third/partner states. The crisis response component has been expanded to include new threats, including cyber threats. The Fund requires participation of actors from different regions, so in the period 2014- 2016 it has already funded a pilot project *Enhancing Cyber Security* (ENCYSEC),[90] which saw Macedonia, Kosovo* and Moldova as the beneficiary countries. The aim of the project was to increase the security and resilience of ICT networks in partner countries through the establishment and training of local capacities to adequately pre-

84 G. Lazarević. IPA II planiranje i programiranje. Mart 2015. Evropski pokret u Srbiji. http://www.rrasrem.rs/doc/2015/RRASREM_IPA_2_mart_2015.pdf.

85 Cybercrime@IPA. Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime. Council of Europe. http://www.coe.int/en/web/cybercrime/cybercrime-ipa.

86 iPROCEEDS. Council of Europe. http://www.coe.int/en/web/cybercrime/iproceeds.

87 Cybercrime@IPA. Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime. Council of Europe. http://www.coe.int/en/web/cybercrime/cybercrime-ipa

88 Assessment report: Criminal justice capacities on cybercrime and electronic evidence in South-eastern Europe. 2013. Data Protection and Cybercrime Division. Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a0d

89 Instrument contributing to Stability and Peace*, preventing conflict around the world. Service for foreign policy instruments. European Commission. http://ec.europa.eu/dgs/fpi/what-we-do/instrument_contributing_to_stability_and_peace_en.htm

90 ENCYSEC. http://www.encysec.eu/web/.

vent and respond to cyber attacks and/or accidental omissions.[91] The specific results set out by the project were: creation and/or development of national CERTs and organizational units/persons available 24/7; adoption of national cyber security strategies and raising of awareness; development of public-private partnerships and international cooperation. Serbia should explore the opportunities that the program has to offer, as well as possible activities that could arise on the basis of this pilot project.

Serbia also has access to the EU Erasmus+ program[92] which includes financing activities aimed at creating knowledge alliances among institutions of higher education, and the development of their capacities. The Erasmus+ program took over these activities from the preceding TEMPUS program, which was discontinued as of January 1, 2014. Within the TEMPUS program, Montenegro, for example, in a consortium of higher education institutions and organizations from Slovenia, Great Britain, Italy and Montenegro, led by the University of Maribor in the period 2013-2016, implemented the project *Enhancement of cyber educational system of Montenegro* (ECESM)[93]. The main goal of the project was to improve, develop and implement standards, guidelines and procedures [in the area of cyber security] at the national level in Montenegro, to allow creation of skilled and professional workforce able to respond to the dynamic e-threats. This goal has been implemented through workshops, presentations and other awareness-raising activities; specialized trainings for different groups - public administration, local administration, private sector, operators/owners of critical infrastructure, small, medium-sized and large enterprises, academic institutions, etc; creating an accredited master program recognized and assisted by the relevant international academic community with the aim of creating highly educated professionals in the area of cyber security.

The **European Defence Agency** (EDA), the body of the EU Council, is another EU unit that deals with the development of capacities in the area of cyber security. Based on the signed Administrative Agreement with this agency, as of 2013 Serbia is able to participate in projects and programs of this EU body[94], although it used this option for the first time in 2016 with the decision to join the project *EU Satcom Market*[95]. Cyber defence is one of the top priorities EDA is engaged in, through capacity building, that is, in the field of research and technology.[96] EDA organizes courses and exercises on cyber security and defence for different levels of decision-makers, as well as projects dealing with raising awareness, development of research agenda in the field of cyber defence, detection of Advanced Persistent Threats, (APTs), protection of information and cryptography.

91 Ibid.

92 Erasmus+ Programme Guide. 2016. European Commission.

93 Enhancement of cyber educational system of Montenegro. ECESM. http://ecesm.net/.

94 Serbia joins EU Satcom Market. 23.3.2016. European Defence Agency. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/03/23/serbia-joins-eu-satcom-market.

95 Ibid.

96 Cyber Defence. 4.6.2015. European Defence Agency. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence.

The increasingly important issue of standardisation has already been opened by ENISA. ENISA's Governance framework for European standardisation also provides recommendations for the standardisation process, that is, it lists which other associated actors should be included. Apart from the industry, public administration, national standardisation bodies, the user community and academia, the framework also states transnational **European Standardisation Organizations** (ESOs) recognized by the European Commission. Among them, it specifically states CEN, the association which brings together national bodies for standardisation from 33 European countries.[97]

CEN membership is based on the principles of one state - one representative and allows a continuous exchange of information and good practices in order to harmonize regional (European) and international (ISO) standards and is not limited to EU Member States. CEN members are thus, for example, Turkey as well as Macedonia[98]. Having in mind the need for implementation of common standards that will only rise as the area of cyber security develops further; Serbia should consider the notion of membership in this association. In fact, the Law on Amendments to the Law on Standardisation[99] was adopted in this regard, in order to comply with Regulation 1025/2012 of the European Parliament and the Council. With the adoption of this Law, the Institute for Standardisation of Serbia, as the only national standardisation body in the Republic of Serbia, now fulfils the preconditions for full membership in European standardisation organizations CEN and CENELEC. CEN membership enables participation in the ETSI CEN/CENLEC coordinating group of experts for standardisation at the European level, i.e. in the CEN-CENLEC focus group for cyber security, as reorganized in 2016, which aims to support the growth of the Digital Single Market, as well as to provide strategic recommendations on standardisation in the area of ICT security, network and information security and cyber security.[100]

One of the newer goals of the EU is to raise awareness of the cyber community on funding opportunities at European, national and regional level, using existing instruments and channels, such as the European Enterprise Network. The Commission, together with the European Investment Bank and the European Investment Fund, will explore ways to facilitate access to resources, for example, through creation of the Cyber Security Investment Platform under the European Fund for Strategic Investments (EFSI). Also, the Commission will explore the possibility of developing a Cyber Security Smart Specialisation Platform in consultation with interested Member States and regions, in order to better coordinate cyber security strategies and establish strategic cooperation between stakeholders in regional ecosystems.[101]

---

97 Governance framework for European standardisation: Aligning Policy, Industry and Research. December 2015. European Union Agency for Network and Information Security.

98 CEN Members. European Committee for Standardisation. https://standards.cen.eu/dyn/www/f?p=CENWEB:5

99 Law on Amendments and Addenda to the Law on Standardisation. "Official Gazette of the RS", No. 46/15. The law came into effect on June 05, 2015.

100 Cyber security. CEN-CENLEC. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

101 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2916) 410 final.

EFSI is currently focused on investments that will help strengthen the economy of the European Union and its Member States. The main goal is to mobilize private investments in order to overcome the existing financing gap in the EU itself in areas such as transport, energy and digital infrastructure, education and training, research and development, information and communication technology, as well as support for small and medium-sized enterprises. EFSI is not an independent body, but is established within the European Investment Bank Group[102]. In this regard, although it is focused on EU Member States, there is a possibility of cross-border cooperation within the EFSI program, while at the same time Serbia, as a state in "the EU enlargement region"[103], fulfils conditions for investments from the European Investment Bank. Accordingly, after the potential establishment of the Cyber Security Investment Platform within the European Fund for Strategic Investments, possibilities for cooperation within the framework of this program should be explored.

NATO

As part of the NATO Science for Peace and Security Programme (SPS), NATO included cyber defence in its key priorities in 2010, based on the Strategic Concept of the Alliance among other things. Within this area, NATO focuses on the issues of protection of critical infrastructure, in terms of development of cyber defence capabilities, capacity building and policies; support for the development of cyber defence capabilities, including new technologies and support for construction of information infrastructure; and raising awareness about the situation in this field[104]. Participation in the SPS program is open to both Member States and partner states. Projects funded under this program are led by a NATO member state, with at least one more partner state. Serbia is actively involved in the program since 2007.

The Ministry of Foreign Affairs of the Republic of Serbia, within IPAP, included activities related to the promotion of the possibilities this program offers and to the creation of a more favourable regulatory and institutional framework that would allow participation of experts and organizations from Serbia within this program.[105] The activities within the program that may be implemented include multi-year projects, trainings and courses (*Advanced Study Institute*, ATI, *Advanced Training Courses*, ATC), as well as workshops (*Advanced Research Workshops*, ARW). This possibility was so far used by countries like Afghanistan, Montenegro

102 European Fund for Strategic Investments – Questions and Answers. Media background document. 26 June 2015. European Investment Bank.

103 EIB provides financial funds to countries of the enlargement region. Enlargement countries. European Investment Bank. http://www.eib.org/projects/regions/enlargement/index.htm.

104 SPS key priorities. 11.6.2012. NATO. http://www.nato.int/cps/en/natohq/85291.htm.

105 Chapter 3.2. Contribution to security through scientific cooperation. Individual Partnership Action Plan (IPAP) of the Republic of Serbia and the North Atlantic Treaty Organization. December 2014. Ministry of Foreign Affairs of the Republic of Serbia.

and Macedonia, for activities such as training of their system/network administrators[106], training on cyber defence for civil servants[107], as well as regional workshops[108].

Currently, Serbia participates in SPS programs related to ABH defence (atomic-biological-chemical defence), the fight against terrorism and the United Nations Security Council Resolution 1325 - Women, Peace and Security[109].

Other NATO programs

As part of NATO's **Smart Defence** concept, the project of Multinational Cyber Defence Capability Development (MN CD2)[110] is currently being implemented. The project leader is Canada, together with five partner countries: Denmark, Norway, Romania and the Netherlands, while Finland has an observer status. Within the project, Canada, Romania and the Netherlands have developed the Cyber Incident Information and Coordination System (CIICS) platform and offered a free pilot version to NATO member states for a period of six months. The main purpose of the program is to facilitate exchange of information related to incidents in cyberspace between national CSIRTs.

The MN CD2 project so far includes three sets of activities: technical information sharing, cyber defence situational awareness and distributed multi-sensor collection and correlation infrastructure. The first two activities are already underway, and the third one has been initiated.[111]

Although the program is primarily focused on NATO member states, requests to take part submitted by third countries are considered on an individual basis - Finland is the first country which has acceded to the mechanism, although it is not a member of NATO. On the other hand, membership in NATO CIICS is open to all NATO member states, partner countries, as well as to certain commercial organizations.[112] Cooperation is realized on the basis of the Memorandum of Understanding.

---

106 The NATO Science for Peace and Security Programme. December 2015. NATO. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151218_151218-sps-eng.PDF.

107 Montenegro. Country Flyer 2016. June 2016. NATO Science for Peace and Security programme. http://www.nato.int/science/country-fliers/Montenegro.pdf.

108 NATO Advanced Training Course – "NATO Regional Summer School on Cyber Defence (NATO RSSCD)". 2013. Faculty of Law. Ljubljana University. http://www.pf.uni-lj.si/media/nato_poster_ohrid.pdf.

109 Country Flyer: Serbia. June 2016. NATO Science for Peace and Security Programme. http://www.nato.int/science/country-fliers/Serbia.pdf.

110 Multinational Cyber Defence Capability Development (MN CD2). https://mncd2.ncia.nato.int/Pages/default.aspx

111 MN CD2 Cyber Defence Capability Development. NATO Communications and Information Agency. https://www.ncia.nato.int/Documents/Agency%20publications/Multinational%20Cyber%20Defence%20(MN%20CD2).pdf.

112 NATO CIICS Federation: A project of the Multinational Cyber Defence Capability Development Programme. 23.10.2015. NATO Communications and Information Agency. https://www.ncia.nato.int/NewsRoom/Pages/151023-NATO-CIICS-Federation.aspx.

Another project within the concept of Smart Defence is focused on multinational education and training in the area of cyber defence (*Multinational Cyber Defence Education and Training Project*, MNCD E&T).[113] The project aims to create a platform for coordinated education and training in the area of cyber defence, and to develop and provide new initiatives that would contribute to filling the gaps in the existing programs of education and development. In addition to enhanced interoperability between NATO member countries in the area of cyber defence, the idea was that within the program, NATO member states and partner countries can, upon completed training, obtain certificates for provision and implementation of similar education programs.

Based on preliminary analyses of currently existing gaps (national, NATO and the EU), it was decided to introduce a certain number of new modules that by their nature allow close cooperation with other NATO *Smart Defence* concept projects, but also the academic community and the industry, such as Cyber Defence Awareness, cyber intelligence, a Cyber Defence International Master and a Master of Law of Cyber Defence and Cyber Security.[114]

The **NATO Cooperative Cyber Defence Centre of Excellence** (NATO CCD CoE) is a NATO accredited centre of knowledge, *think-tank* and centre for training. NATO CCD CoE is focused on interdisciplinary applied research and development, as well as on consulting services, training and courses in the field of cyber security. The Centre is neither a part of the NATO command structure nor financed from the NATO budget. Instead, member states provide contributions to its budget.

The Centre's mission is to build capacity, cooperate and exchange information between NATO, member states and partners in cyber defence. The Centre brings together experts in this area, from legal scholars to experts in strategy, as well as technology researchers with previous experience in the military, state administration and industry. Membership is open to all member states, but also to countries that are not a part of NATO, as a contributing partner, such as Austria and Finland, which means that participation is open to Serbia as well.[115]

ITU-IMPACT

ITU is the most active organization dealing with the issue of cyber security at the international level, especially when it comes to developing security frameworks and standards. Based on the **ITU Global Security Agenda** (GCA), in 2011 the Union published a National

113 Multinational Cyber Defence Education and Training Project, MN CD E&T. http://www.mncdet-pt.net/. In Portuguese language.

114 Iniciativas de Educação & Treino. Multinational Cyber Defence Education and Training Project (MNCD E&T). http://www.mncdet-pt.net/#!et-iniciatives/cc2z.

115 NATO Cooperative Cyber Defence Centre of Excellence. Estonian Defence Forces. http://www.mil.ee/en/landforces/CCDCOE

Cyber Security Strategy Guide[116], which serves as a starting reference for the development of national cyber security strategies. The guide was prepared in cooperation with major international organizations in this area, as well as with representatives of the industry, civil society organizations and the academic community. The ITU, in partnership with a number of relevant organizations such as the World Bank, UN Conference on Trade and Development (UNCTAD), Organization for Economic Co-operation and Development (OECD), NATO CCD CoE, ENISA, Microsoft, Oxford University, and others, is currently working on the development of the Guide for Development of National Cyber Security Strategies. The guide will contain clear information in terms of the importance and content of national strategies, but also in terms of mapping relevant models, as well as the support available from various organizations in the process of development of such a document.[117]

Likewise, within the ITU Global Security Agenda, in relation to the fifth goal - international cooperation – in 2008 the Union established a partnership with the **International Multilateral Partnership Against Cyber Threats** (IMPACT) in order to share expertise and resources to detect, analyze and respond to cyber threats across the 193 ITU member states. The partnership aims to establish a platform for cooperation of states, industry, the academic community and executive authorities in the development of cyber security strategies and strengthen coordination and cooperation in the field of security of cyber space.[118] The partnership provides a range of services in the areas of technical and non-technical support, as well as activities aimed at development and capacity building. With the support in establishing national CERTs, the partnership is also active in organizing cyber drills. Serbian representatives from RATEL and the Ministry of Interior took part in one such exercise organized in 2015 in Montenegro.

In this respect, the **ITU-IMPACT coalition** is particularly important for countries that do not have sufficient resources to establish their own cyber response centres. An example of effective use of the opportunities that this partnership offers is Montenegro, which so far carried out, with the support of ITU-IMPACT, an analysis of threats in Montenegro's cyber space[119], developed a strategy for the establishment of a National CIRT in Montenegro, and carried out an analysis of critical information infrastructure, based on which the Methodology for selection of critical information infrastructure[120], as well as the accompanying action plan for its implementation, were developed.

116 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

117 National Strategies. ITU. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.

118 A. Ntoko. 2011. Global Cybersecurity Agenda (GCA). A framework for international cooperation. ITU. https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf.

119 Analysis of Threats in Cyber space of Montenegro. 2014. Ministry of Information Society and Telecommunications. The Government of Montenegro.

120 Methodology of Selection of Critical Information Infrastructure. 2014. Ministry of Information Society and Telecommunications. The Government of Montenegro.

Therewith, the **IMPACT Training and Skills Development Centre** conducts training programs in cooperation with companies and institutions such as the ITU, SANS Institute, E-Commerce Consultants, and the Honeynet project.[121]

Serbia is a member of the ITU and at the same time has access to services provided by IMPACT in the field of cyber security.[122]

UNITED NATIONS

In 2013, the UN Office for Drugs and Crime (UNODC) and the ITU suggested that the United Nations Development Programme (UNDP) becomes the leading agency for program support in the area of cyber security, which is provided to developing countries (which have to ask for this assistance from the UN).[123] Thus, since 2014 UNDP provides services to states in the area of cyber security in the form of training workshops, assessments and overcoming risks, building capacities to respond to incidents, resilience, development and evaluation of policies and standards related to cyber security and certification by ISO 27001 standards.[124] In the Western Balkans, until now, this option has been used by Macedonia, where UNDP has already provided support to state institutions in reforms related to the security system within the EU accession agenda. Within this framework, special focus has been placed on the development of a National Cyber Security Strategy, whereby UNDP has offered assistance in the preparation of the Study on the assessment of conditions for development of a national cyber security strategy.

In the area of information technology, Serbia is currently using UNDP resources within the Open Data initiative, which is, in cooperation with the World Bank, being implemented by the Ministry of State Administration and Local Self-Government.[125]

121 IMPACT Training and Skills Development Centre. IMPACT. http://www.impact-alliance.org/services/centre-for-training-overview.html.

122 Countries. IMPACT. http://www.impact-alliance.org/countries/alphabetical-list.html.

123 UNDP Cybersecurity Assistance for Developing Nations. 18.4.2016. CSO50 Confab. UNDP. http://www.csoconfab.com/wp-content/uploads/2016/03/CSO50_2016_Paul-Raines_Providing-Effective-Cybersecurity.pdf.

124 Ibid.

125 Open Data: Open Opportunities. 12.1.2016. UNDP in Serbia. http://www.rs.undp.org/content/serbia/en/home/ourperspective/ourperspectivearticles/open-data--open-opportunities.html.

VI PUBLIC-PRIVATE PARTNERSHIP

In the international sphere, public-private partnership is increasingly turning into a type of mechanism necessary for the development of an efficient framework for cyber security. This sort of approach enables timely exchange of information between all relevant actors, as well as responding to risks, threats and incidents, if such should occur. Apart from that, public-private partnership opens the doors for the exchange of knowledge and experience, as well as good practice examples.

In 2014, **NATO** launched the *NATO Industry Cyber Partnership* (NICP) as a platform which relies on existing NATO structures including various NATO authorities, the national CERTs and representatives of the industry, including small and medium enterprises in NATO member countries. The significance of participation of academic communities has also been acknowledged. The formation of the platform was previously supported by all 28 member countries at the NATO Summit in Wales as a mechanism which recognizes the significance of cooperation with partners in the industry for the purpose of realizing NATO's goals in the field of cyber defence policy. One of the goals of the platform is to enable participation of the industry in multinational projects of *Smart Defence*. Thus, NATO is using the resources which the cyber security industry has to offer, in regard to improving cyber defence in NATO's defence department chain of supply; support to NATO programmes of education, training and excercises in the area of cyber defence; exchange of information, experiece and knowledge; and creation of efficient and adequate support in case of cyber incidents.[126]

In July 2016, the **European Commission** adopted the framework agreement for public-private partnership for industrial research and development in the area of cyber security at the EU level. Public-private partnership refers to the cooperation of the European Commission and the Stakeholder Organisation. The decision of the Commission specifies that further development of activities aimed at research and development in the area of cyber security, carried out within private-public partnership, shall be provided through the EU's Horizon 2020 programme, within the activity titled "*Cluster facilitated projects for new industrial value chains*"[127]. The Stakeholder Organization has, for the purpose of the

126 NATO Industry Cyber Partnership. NATO. http://www.nicp.nato.int/index.html.

127 Commission Staff Working Document. Contractual Public Private Partnership on Cybersecurity & Accompanying Measures Accompanying the document Commission Decision on the signing of a contractual Arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. SWD(2916) 216 final.

agreement, been defined as the European Cyber Security Organisation (ECSO).[128] ESCO is the contractual counterpart to the Commission, led by the industry, for the implementation of the contractual arrangement of public-private partnership in the field of cyber security. The primary goal of ESCO is to support all of initiatives and projects, the goal of which is the development, promotion and support of European cyber security, aimed at:

- Foster and protect from cyber threats the growth of the European Digital Single Market;
- Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position;
- Develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.[129]

ESCO members encompass a wide range of stakeholders, such as large companies, small and medium enterprises and start-ups, research centres, universities, clusters and associations, as well as local, regional and national administrations of EU member states, states which are part of the European Economic Area (EEA) and the European Free Trade Association (EFTA), as well as partner countries within the EU's Horizon 2020 programme.[130] Serbia, being an associate country within the Horizon 2020 programme, has access to ESCO and therefore meets the requirement for participation in programmes of the contractual arrangement of the EU public-private partnership in the field of cyber security.[131]

The EU's Global Strategy on Foreign and Security Policy provides for the response of the EU to cyber challenges to be set within a framework of a strong public-private partnership. In that sense, cooperation and exchange of information is emphasized, among member states, institutions, the private sector and the civil society, for the purpose of cultivating the common culture of cyber security and raising awareness on possible cyber disruptions and attacks. The chapter on partnerships states that global management of issues in the field of cyber, relies on the progressive alliances among states, international organisations, industry, civil society and technical experts.[132]

Within further strengthening EU resilience in the field of cyber security, the Commission aims to establish a high-level advisory group which shall comprise of the experts and decision-makers, industry representatives, academia, civil society and other relevant organisations. The role

128 Commission Decision of 5.7.2016. on the signing of a contractual arrangement on a public-private partnership for cyber security industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. C(2016) 4400 final.

129 European Cybersecurity Organisation. http://www.ecs-org.eu/about

130 European Cybersecurity Organisation. http://www.ecs-org.eu/membership

131 Associated Countries. H2020. European Commission Directorate-General for Research and Innovation. http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/3cpart/h2020-hi-list-ac_en.pdf

132 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy. June 2016. European Union.

of the group shall be the provision of external expertise and suggestions for future steps of the Commission, in regard to strategic documents in the field of cyber security.[133]

Being a private company **Microsoft**, through its Microsoft EU Government Affairs, works with state administrations, the industry and the broader business community, as well as with the civil society, on advocating public policies that coincide with the interests of the company. This sort of approach is applied in line with the company's Public Policy Agenda, which, among its goals for 2016, specifies the maintenance of trust in IT, by maintaining the balance between national safety, privacy rights and personal freedoms; encourage responsible leadership in regard to the government policies that can encourage businesses to adopt principled approaches to conducting business and to uphold their public responsibilities; as well as the strengthening of efforts to fight cybercrime through the Microsoft Cyber Crime Center which offers access to expertise and cutting-edge tools, for the purpose of making the Internet and protecting consumers online.[134]

Within the mechanism for cooperation with states, Microsoft has, way back in 2003, established the Government Security Program (GSP) within which it cooperates on specific issues of security with over 30 governments in the world. The programme, among other things, provides users with controlled access to the source codes for important Microsoft programmes, which enables governments to evaluate existing systems; technical information on Microsoft products and services, which helps governments design, develop and implement more secure computing systems; as well as vulnerability and threat intelligence, so that governments respond more efficiently and efficiently to incidents. This reduces the possibility of cyber attacks, through exchange of security intelligence data, which Microsoft collects on cyber threats and malicious software. This information includes the known weakness which Microsoft is investigating, upcoming and released software patches, information on incidents and the like.[135] This area of the GSP programmes could help (among other things) the process of establishing the national CERT in Serbia, bearing in mind that Microsoft already operates in the country and monitors incidents which occur in its cyber space. This is the case, in particular, if it turns out that the anticipated national CERT lacks the sufficient capacities.

***

Accordingly, although not yet officially, the existence of public-private partnerships, apart from the objective advantages it brings, tends to become, in the near future, an official obligation when it comes to the international bodies and organisations in which Serbia participates, whose member it wishes to become and/or with which it actively cooperates.

---

133 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2016) 410 final.

134 2016 Global Public Policy Agenda: Real Impact for a Better Tomorrow. Microsoft. https://www.microsoft.com/about/csr/downloadhandler.ashx?Id=03-06-01.

135 Government Security Program Backgrounder. September 2014. Microsoft Corporation. http://download.microsoft.com/download/B/C/A/BCAFF3F5-5DB5-4AB4-9AAB-5CF0814E0948/GovernmentSecurityProgram.pdf

Therefore, it is necessary to consider the possible mechanisms for establishing public-private partnership in the field of information security.

THREE POSSIBLE SCENARIOS FOR ESTABLISHING PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF INFORMATION SECURITY IN THE REPUBLIC OF SERBIA

The establishment of a substantial public-private partnership is a lasting process, depends on all actors participating in it and is primarily based on the trust they mutually develop. Given that the concept of cooperation between the state, the private sector, the academic community and the civil society is increasingly becoming a standard model for the development of policies, technical solutions and responses to incidents in the area of information security, the scenarios in which a powerful and efficient mechanism of public-private partnership can be developed in Serbia needs to be considered, what are the prerequisites and what are the possible obstacles standing in the way. The presented scenarios include natural development of the public-private partnership through cooperation of CERTs, formalisation of public-private partnership within a specific authority, but also cooperation forced by a specific incident taking place within national ICT systems. It is necessary to stress that these are only some of the possible models of development of PPPs on the national level, but also, that these are not mutually exclusive, and that they can develop and/or occur simultaneously and as such can be complementary.

Scenario 1: Natural development of public-private partnership through cooperation of CERTs

One of the legal roles of national CERTs is the maintenance of records of special CERTs, i.e. CERTs within a specific legal entity, a group of legal entities, field of operation and similar. The national CERT, therefore, also has a role in the cooperation between the public and the private sector, being a central point of connecting existing CERTs within a state.

The role of special CERTs is for each of them to develop in their own field, that is, to "cover" the area for which the team, comprising a specific CERT, is specialised. This implies various areas of industry, financial institutions, statutory authorities, civil sector, academy

and the like. Apart from capacity building and the expertise for monitoring developments in the area for which a CERT is specialised, capacities also need to be built for cooperation between existing CERTs. The national CERT is a good starting point for directing information, knowledge and good practices.

Primary cooperation of special CERTs (regardless of whether they are public or private) should develop both at the technical and the expert level. This cooperation is based on the principle of allocating resources between CERTs which have different capacities and area of expertise. Also, this implies the sharing of knowledge, relevant and current information and experience.

Bearing in mind that it is unrealistic to expect from the state to provide resources for the formation of CERTs which would cover every single area of the system, the importance of the public-private partnerships is immeasurable, especially at the level of technical and expert cooperation – in regard to rationalisation of resources.

The following degree of cooperation of private CERTs is cooperation at the policy level. Given that Serbia is still at the beginning of establishing private CERTs and that experience, in the formal sense of the word, is therefore not vast enough to define the specific challenges in the work of CERTs at the policy level, there is a possibility of forming some sort of a community of private CERTs which would enable the creation of common policies and recommendations for the improvement of the formal and technical aspects of operations. This would ensure easier cooperation with the state, at the policy level, given that it would enable joint action, based on specific experience and practice, which CERTs have developed during their work, as well as on the proposal of policy solutions, based on common interests.

This scenario represents a natural evolution of public-private cooperation, which, starting from the technical level, in time, encompasses other aspects of information security issues and prevention and response to risks, all up to the level of policies. On the other hand, the major risk to the development of an effective public-private partnership carried by this scenario, is to have cooperation remain at the technical level, given that it most certainly is necessary, and that it has been prescribed by the Law. Without significant political will, from both the public and the private side, there is a risk that the "*spill-over effect*" might actually never occur and that this scenario would not, in the long term, contribute to comprehensive public-private cooperation, neither at the technical nor at the policy level.

Scenario 2: Formal and legal public-private partnership within the Coordination Body

Another possibility for the development of public-private partnership in the field of information security, is created through the establishment of the Body for the Coordination of Information Security. It has already been mentioned that the Coordination Body represents an indication of the political will (or at least, the lack of resistance) towards formation of public-private partnerships, through the space envisaged for the formation of expert working groups for specific issues of information security.

In that sense, in order to ensure a continuous, formal and legal private-public partnership in the area of information security in the Republic of Serbia, the possibility of establishing a permanent expert working group within the Coordination Body should be considered, given that the legal basis, for something like this already exists. The permanent, expert working group would serve as a forum for the exchange of knowledge, experience and information, i.e. connecting relevant actors from the public and private sector, but also of the academic community and the civil sector. Bearing in mind that the Law on Information Security prescribes that the envisaged expert working groups are formed for the purpose of improving specific areas of information security, the proposed Permanent Expert Working Group could have the main role of monitoring the implementation of the Law, as well as of the pending Strategy and Action Plan, but also to take part as an advisory body in the process of creating future documents in this field.

The main obstacle for this scenario is the current, insufficiently defined position of the Coordination Body, which also entails the issue of the specific role and the manner of functioning of the envisaged expert working groups. Accordingly, in order for the proposed model of development of public-private partnership to be possible, the role and position of the Body for the Coordination of Information Security needs to be clearly legally defined, and the possibility of formal and legal establishment of a body which would function as the proposed Permanent Expert Working Group, gathering representatives of the relevant state institutions, other governmental bodies, the private sector, the technical and the academic community and the civil sector needs to be considered.

Scenario 3: Forced cooperation

The third scenario implies a situation in which no steps are made towards the formation of such mechanism, until some specific incident, of a larger scope, occurs. Bearing in mind that the area of information security has only begun developing, as well as the formation of a national centre for the prevention of security risks in ICT systems, there is a great possibility for the capacities which are still being developed to be insufficient for an adequate response to a specific incident. In that case, the state could/should rely on the support of private CERTs in the defence against an attack and/or in overcoming the consequences of one, therefore being forced to cooperate with the private sector.

This is the worst case scenario in regard to the possible models of development of public-private partnerships, which undoubtedly and primarily incurs losses – regardless of whether it is a case of data, interference of normal functioning of the state's information space or simply the loss of confidence in the ICT systems and services provided by the state. On the other hand, although the least favourable one, this scenario could contribute to an accelerated generation of the necessary political will for the formation of public-private partnership, based on a practical example, a direct demonstration exercise, on the capacities, experience and possibilities which the private sector is able to offer.

VII CASE STUDIES ON POSSIBLE SOLUTION IN SPECIFIC AREAS OF INFORMATION SECURITY

Although national strategies of cyber security do not differ much in their basic assumptions, depending on the strategic orientation and the available capacities, states choose to place specific focus on different areas. Depending on the level of cyber security development, the intended measures may be short-term, medium-term and long-term. In the case of states which are in their initial phases of the development of the cyber security concept, measures will refer to the direct establishment of its basic mechanisms, whereas states with a higher degree of security in this field use the existing mechanisms for the fulfilment of other strategic goals, such as the strengthening of national economy. Further in text are several examples of development of various areas of information security, along with a description of the possible mechanisms which certain states used for the fulfilment of their strategic goals.

Critical Information Infrastructure

The Directive concerning measures for a high common level of security of network and information systems across the EU (the NIS Directive) prescribes that member states are obliged to identify their critical information infrastructure, or more precisely, ICT operators of special importance, and to adopt measures at the national level which determine to which bodies the provisions of the Directive at hand apply to. Although the NIS Directive also contains a list of the most common, operators of special importance, the principle of identifying these actors needs to be applied to the national frameworks, bearing in mind the specific circumstances in each country respectively. One possible obstacle standing in the way of this process is the fact that some states do not yet have a regulated field of critical, that is, infrastructure of special importance in its general sense, a prerequisite for determining the information infrastructure of special (essential) importance. However, there are examples where this formal obstacle has been surpassed in practice, within similar normative circumstances in which Serbia finds itself at this moment.

Namely, the Cyber Security Strategy of Montenegro[136], adopted in July 2013, specifies, as one of the primary goals, the "protection of the critical information infrastructure". It is important to mention that Montenegro – just like Serbia – has no officially defined critical infrastructure, but the state has, nevertheless, found a way to use the available mechanisms and resources and to commence work on definition and protection of the critical information infrastructure (CII), just as the Cyber Security Strategy has envisaged. When preparing the Report on the assessment of state of affairs in the cyber space of Montenegro[137] for the need of establishing a National CERT team, the competent Ministry - Ministry for Information Society and Telecommunications (MIST) –prepared an overview of the critical sectors in Montenegro, for the purpose of identifying critical information infrastructures. For the needs of this project, MIST has, in cooperation with the ITU-IMPACT, headquartered in Malaysia, developed a Methodology for the Identification of Critical Information Infrastructures[138].

The Methodology, accompanied by an Action plan, emphasizes the need to define the key holders of critical information infrastructures, as well as to identify the property, processes and services which fall within the critical information infrastructure and to compile a final CII list. The methodology comprises of the following steps:

6. Preparation of the list of critical infrastructure sectors in Montenegro in cooperation with IMPACT and based on international criteria;

7. Identify the holders of the critical information infrastructure within the identified bodies/authorities;

8. Define the sub-sectors and critical service/product operators in cooperation with the holders of the sectors – such as the private financial infrastructure and banks; the production, transfer, management systems and electrical energy distributers and providers; healthcare services, ambulances, hospitals and public and private healthcare institutions and the like;

9. Design and disseminate a questionnaire to critical service and product operators, for the purpose of analysing the degree of criticality of services and products, their dependency on ICT and the possibility of interrupting operations due to a cyber attack.

Based on the collected information, the final list of critical information infrastructure of Montenegro is created, as part of the international critical information infrastructure, in

136 The Cyber Security Strategy of Montenegro. 2013. Ministry of Information Society and Telecommunications of Montenegro.

137 Report prepared in cooperation with IMPACT from Malaysia. The report contains the information on activities carried out by ITU/IMPACT in Montenegro, so as to have an overview of the entire analysis of the situation in cyber space. The analysis of threats in cyber space of Montenegro. Ministry of Information Society and Telecommunication of Montenegro.

138 Methodology of Selection of the Critical Information Infrastructure. 2014. Ministry of Information Sociecty and Telecommunications of Montenegro.

line with international standards, and harmonized with the provisions of the NIS Directive, which refers to all EU member states.

This is not an isolated example of using available mechanisms for capacity building and development in the field of cyber security in Montenegro. Being the regional leader in the use of available forums and resources for the development of its own capacities, Montenegro has, so far, organised a number of trainings for employees working in the field of cyber security, within the National CERT and the local CERT teams in cooperation with the ITU and IMPACT, as well as through the IPA funds of the European Union, the NATO Science for Peace and Security program, but also through bilateral cooperation with states, such as Japan. The ITU has also helped organise a regional conference within the annual Festival of Information Technology Achievements (INFOFEST) in 2015, whereas in 2014, Montenegro conducted this activity in cooperation with the Central Bank.[139]

Serbia, being a member of the ITU and IMPACT, as a candidate state for membership in the European Union and a NATO partnership state, through mechanisms of the Individual Partnership Action Plan and membership in the NATO Science for Peace and Security Program, also has access to the aforementioned mechanisms and resources.

Capacity building and development in the field of cyber security

Capacity building, in particular long-term education programmes, are one of the basic elements specified in the guidelines for writing national cyber security strategies of various international bodies and organisations. Apart from ensuring a platform for more efficient and comprehensive national mechanisms for cyber security, investing into future generations of experts contributes to the position which a specific country might aim to take in the field of cyber security in the future. Strategic investment into the development of capacities and capabilities in the field of cyber security has a positive effect on the transformation of the labour market, which has to respond to the envisaged families of new occupations in the upcoming decades[140], and in particular to an increasing need for a qualified workforce in this field, pertaining to the offer of the labour market[141]. Although the development of educational programs dealing with the issues of cyber security, both at a technical as well as at the political

---

139 Report on realization of activities from the action plan for implementation of the Cyber Security Strategy in Montenegro for the period 2013-2015. 2015. Ministry of Information Society and Telecommunications of Montenegro.

140 The Report of the World Economic Forum *The Future of Jobs* from early 2016 identifies the jobs related to computer and mathematical sciences, including information security, as one group of jobs which would be in focus in the following decade
The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution. Global Challenge Insight Report. January 2016. World Economic Forum. http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.

141 In 2015, Frost and Sullivan concluded that the global lack of employed professionals in the area of cyber security is a result of a very limited offer on the labour market and they were able to estimate that by 2020 the demand of the global market would be over one and a half million of professionals.
M. Suby & F. Dickson. The 2015 (ISC)2 Global Information Security Workforce Study. April 2015. Frost & Sullivan White Paper. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

level, requires significant investments and resources, there are, at the same time, numerous programs and funds, which make these aspirations more easily attainable.

Finland, for example, which bases its approach to cyber security on three pillars: public management and administration, economy and industry and academy and research, as a primary goal within the Cyber Security Strategy, suggests a vision of the state as a leading country in the field of cyber security – by strengthening the research and development elements in this field, as well as education at all levels. Activities aimed at education of various groups in society are defined as the fundamental element for capacity building of various sectors in the society, in the field of cyber security. The programme for the implementation of the Finish Cyber Security Strategy states that universities shall be the key actors for strengthening the prerequisites for basic and applied research and innovation in the field of cyber security at the national and international level[142]. The accompanying document of the Cyber Security Strategy defines that cyber security is to be introduced as a subject at all levels of education. Universities have a role in strengthening the tools for basic researches, applied research and innovations in the field of cyber security, whereas universities of applied sciences are focused on the improvement of prerequisites for product development.[143]

In that sense, the state has launched several programmes of cooperation with universities. The Ministry of Education and Culture has established a program OKMICT – 2015 which is primarily focused on the consideration of ICT profiles and university capacities. Also, based on the report of the ICT 2015 working group, the Academy of Finland has, together with the Agency for Financing Innovations of Finland, initiated a common program for research, development and innovations ICT 2023, the aim of which is further strengthening of expertise in the area of processing of the, so called, deep data.[144]

Apart from the significant national resources which Finland ensured for investments in this field, the state is also making efficient use of other available programmes, such as the resources provided by the European Union. In that sense, the Innovative Cities programme 2014-2020 (INKA) was developed, within which the Jyväskylä[145] region was chosen for the establishment of the research, development and education centre JyvSecTec (Jyväskylä Security Technology) in the field of cyber security[146]. The INKA program developed by the Funding Agency for Technology and Innovation, (TEKES), including the ministries of economy and employment, aims at the development of a national network of education, research and industry, as well as at international activities, for the purpose of supporting capacity building and new economic possibilities in this field.[147] Apart from the investments

142 The Implementation Programme for Finland's Cyber Security Strategy. 11.3.2014. The Security Committee.

143 Finland's Cyber Security Strategy. Background dossier. Secretariat of the Security and Defence Committee.

144 The Implementation Programme for Finland's Cyber Security Strategy. 11.3.2014. The Security Committee.

145 Jyväskylä. http://www.jyvaskyla.fi/international

146 The JyvSecTec Centre is to a large extent used also by the Finnish defence forces for preparation for the NATO exercie Locked Shield – the largest and most advanced international cyber defence exercies.

147 M. Lehto. Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities. In N. Abouzakhar. 2015. ECCWS2015 – Proceedings of the 14th European Conference on Cyber Warfare and Security 2015. Academic Conferences Limited.

provided to the region by TEKES, this region has entirely used the possibilities provided by the EU structural funds. Specifically, Finland has relied on the Smart Specialisation Platform (S3 Platform)[148] of the European Commission aimed at research and innovation strategies for smart specialisation (RIS3), directing the resources towards modernisation of the economic structure by capacity building of universities. European structural funds thus also support research programmes at the Jyväskylä University, whereas for the Jyväskylä University of Applied Sciences, they are the major, individual source of funding for research and development programmes. Other external sources of financing include ministries, municipalities, foundations and the private sector.[149]

The Jyväskylä University is the pioneer in the development of master programs in the period 1995-2000, also with the support through EU structural funds. The first master programs in the field of information technologies had a great impact on further development of the Jyväskylä region in this field and thus, in 1998, the Faculty of Information Technologies was founded. Today, the Jyväskylä University also runs a two-year master programme in English, aimed at decision-makers and the middle management, whereas a large number of other Finish universities and research centres, such as the Aalto University, the Oulu University, the Tempere Technological University, the VTT Technical Research Centre of Finland as well as the aforementioned Jyväskylä University, have been involved in comprehensive joint projects in the field of cyber security, financed through EU funds. Examples include EU projects such as ECOSSIAN (European Control System Security Incident Analysis Network)[150] and SASER CelticPlus[151] within which the VTT Technical Research Centre of Finland, being a member of consortium, along with companies from Finland and other parts of Europe, participates in projects focused on issues such as the protection of the critical infrastructure and the global initiative for cyber security, industrial control systems and smart networks, Cloud Computing and Big Data.[152]

Other developed countries too, especially European ones, place capacity building and education in the field of cyber security in focus. Since 2011, the German Ministry of Education and Research, in cooperation with the Ministry of Interior and the private sector, has been supporting a group of educational centres for cyber security which is part of a wider network of the Fraunhofer-Gesellschaft Institutes[153]. France has used the renowned universities in Bretagne, so as to develop a centre of excellence. Estonia has created the HITSA Innovation Centre (*Hariduse Infotehnoloogia Sihtasutus*)[154] as a public-private partnership between the Ministry of Education and universities on one side, and private ICT companies on the other. The Austrian Agency for the Promotion of Research has entered into partnership with the Institute for Technologies (AIT) for the purpose of promoting cooperation with

148 European Commission Smart Specialisation Platform. http://s3platform.jrc.ec.europa.eu/

149 K. Mukkala, J. Ritsilä and E. Suosara. OECD/IMHE – Supporting the contribution of higher education institutions to regional development. Self-evaluation report of the Jyväskylä region in Finland. 2006. Ministry of Education, Finland. 2006:26. https://www.oecd.org/finland/36175211.pdf

150 ESOCCIAN. http://ecossian.eu/

151 SASER CelticPlus. https://www.celticplus.eu/.

152 The Implementation Programme for Finland's Cyber Security Strategy. 11.3.2014. The Security Committee.

153 Fraunhofer Institute for Secure Information Technology. https://www.sit.fraunhofer.de/en/.

154 Innovation Centre. http://www.innovatsioonikeskus.ee/en.

the ICT industry, as well as the SBA Research centre, the largest Austrian centre of excellence in the field of information security, developing researches and conducting trainings for the public and private sector in cooperation with numerous private companies.[155]

Serbia has access to some of the resources which Finland and other countries used in their process of modernisation of the educational system. For example, Serbia belongs to the group of countries which have been registered within the S3 platform, although it is not an EU member state.[156] ICT has been specified as one of the seven defined priority areas within the RIS3 mechanisms for Serbia[157], and therefore it could use this structural fund within the Smart Specialisation Strategy, for capacity building of the educational system for education and development of prerequisites for strengthening national cyber security. Horizon 2020 is also a powerful financial mechanism, within which institutions, universities, organisations and companies from Serbia can participate as part of a consortium with European partners, which, at the same time, is an excellent opportunity for exchange of experiences.

Strengthening of the national economy through safe cyber space

The increasingly powerful trend of transferring to electronic business implies that a safe cyber space provides the basis for further development and strengthening of the national economy. At the same time, while there is a growing need to respond to the risks in cyber space throughout the world, there is also the potential for development of the industry which will provide such a response, and thus ensure market competitiveness. Many developed countries, and more often even developing ones, have recognised this potential and have entered into public-private partnerships which include the ICT industry, as well as other actors, such as the insurance industry, for the purpose of strengthening security of the national cyber space, but also to reinforce the economy through the use of innovative industries.

Thus, for example, the Security Strategy of Great Britain has, since 2010 defined attacks on the national cyber space, as a Tier One threat, i.e. as one of the highest priority risks to national security.[158] The Security Strategy from 2015 has confirmed this trend, anticipating further investments into the field of cyber security, as a branch largely contributing to

155 V. Radunović & D. Rüfenacht. Cyber security Competence Building Trends. Research Report. February 2016. DiploFoundation. https://issuu.com/diplo/docs/cybersecurity_full_report.

156 V. Radunović & D. Rüfenacht. Cyber security Competence Building Trends. Research Report. February 2016. DiploFoundation. https://issuu.com/diplo/docs/cybersecurity_full_report.

157 Serbia. European Commission Smart Specialisation Platform. http://s3platform.jrc.ec.europa.eu/regions/RS/tags/RS

158 A Strong Britain in an Age of Uncertainty: The National Security Strategy. 2010. HM Government. Crown Copyright 2010.

the British economy.[159] Both strategies emphasize that the establishment of an adequate, comprehensive system of cyber security is at the same time an enormous possibility for Britain to use the economic potential of comparative national economic and security advantages, to make Britain the world leader in its field.

Accordingly, Britain has within its concept of understanding cyber security set the goal of ensuring a stable and strong economy in first place, ahead of national security in its traditional sense. The British Cyber Security Strategy, as its primary goal, specifies promotion of the United Kingdom as one of the most secure places in the world to do business in cyber space, whereby the private sector is a natural partner of the Government and the state's legislative bodies in the exchange of information and resources, joint response to challenges and the prevention of threats in cyber space. By protecting British intellectual property and incomes, the state has decided to also include companies which cannot be directly defined as a critical infrastructure, into the framework of protection provided by the Centre for the Protection of National Infrastructure. The Cyber Hub was developed as well, as a public-private project in which the state and the private sector forward information on threats to nodes in key economic sectors, for the purpose of establishing prevention mechanisms and exchange of good practices.[160]

Defining the field of cyber security as business risk of priority importance for national security resulted in the cooperation of the Department for Business Skills and Innovation with the private sector, including also, the insurance market (more broadly, insurers, lawyers and auditors).[161] The key result of this cooperation is the defining of minimal cyber security standards within the Cyber Essentials scheme[162] which provide clear guidelines for the basic technical controls which all organisations and companies, small and medium enterprises above all, should apply so as to reduce the risk of common threats lurking from cyber space. The idea of the programme is to enable British companies to achieve a competitive advantage against others who do not manage cyber risks in an adequate manner – all for the purpose of strengthening the national economy.

Within the programme, the state also issues certificates on the existence of a basic level of protection, that is, a qualification to companies to be used when addressing clients, creditors and insurance companies, confirming that they have undertaken the basic precautions against cyber risk. Since October 2014, possession of the certificate has become the necessary prerequisite for all agreements which the central government enters into with the private sector in the area of managing sensitive and personal data and ICT systems.[163] In this way, the state has conditioned the private sector to introduce the minimal standards

159 National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. 2015. HM Government. Crown Copyright 2015.

160 The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. 2011. Cabinet Office. Crown Copyright 2011.

161 The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. 2011. Cabinet Office. Crown Copyright 2011.

162 Cyber Essentials. http://www.cyberessentials.org/

163 The UK Cyber Security Strategy 2011-2016. Annual Report. April 2016. Cabinet Office. Crown Copyright 2016.

of cyber security which it has itself prescribed, ensuring thus the initial prerequisite for the creation of a more secure British cyber space.

In a Joint statement of the Government and the insurance industry, the important role of cyber insurance in helping firms outside of the critical national infrastructure to manage of cyber risks efficiently is highlighted; through promotion of the adoption of good practice, including Cyber Essentials, which insurers will consider as a component in the risk assessment for small and medium enterprises.[164]

Some insurance companies have already developed policies which provide cyber insurance for small and medium enterprises that include the price of Cyber Essentials certification, for the purpose of reducing the cost which accreditation entails – thus ensuring lower premium prices paid for insurance itself. The leading insurance companies in Britain - Lloyd's, Association of British Insurers (ABI) and the British Government have agreed on the need to create a cyber insurance guide, cooperation on the establishment of a forum for the exchange of data and opinions, and consideration of possible scenarios of cyber catastrophes.[165]

Cooperation of the state and the insurers will further be strengthened through the Cyber Security Information Sharing Platform (CiSP) established within the CERT-UK, for the purpose of strengthening the general awareness on cyber threats and reducing their impact on the British economy.[166]

Britain is a practical example how focusing on the economic potential provided by a higher level of cyber security enabled the development of other sectors. The Government developed the basic guidelines for cyber security and established a certification programme. The development process itself, the participation of the insurance industry, has ensured support of a part of the private sector for this initiative. Concurrently, also led by the principle of business development and strengthening, British companies introduced these guidelines so as to reduce the premiums which they pay for insurance of its business operations on the one hand, and in order to retain consumer confidence and attract new clients based on their certified guarantee of cyber security, on the other.

On the other hand, the programme also helps insurers to make a clear difference between the risks on the market of small and medium enterprises, bearing in mind that it has been emphasised that not even the insurance societies have developed the market of cyber insurance in its entirety, due to the lack of clearly defined threats and possible scenarios,

164 Joint Government and industry statement on the cyber insurane market. 5 November 2014. Gov.uk. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf

165 UK Cyber Security: The role of insurance in managing and mitigating the risk. March 2015. HM Government and MARSH.

166 Cyber-security Information Sharing Partnership (CiSP). CERT-UK. https://www.cert.gov.uk/cisp/

which is why among some, this field is present only within expanded insurance packages – which do not cover all of the possible incidents – and not as a separate concept.[167]

Since the Cyber Essentials scheme was initiated, the state has, through the CREST accreditation body, issued over 2,000 certificates, including certificates to FTSE 100 organisations (*Financial Times Stock Exchange 100 Index*, FTSE 100)[168]. This serves to prove:

- The success of a state in prescribing minimal cyber security standards;
- The fact that even the strongest companies pay attention to this issue and agree with the policy of prescribing the minimal standards;
- The results which a state can achieve in cooperation with various actors in the private sector, in the effort to realize the set goals, related to cyber security;
- The fact that the issue of cyber security is becoming increasingly comprehensive and that in that sense it is necessary to be aware of the fact that the cyber element is the one permeating all aspects of life – the security, political, economic, educational, but individual as well.

Britain has even gone a step further in the sense that it no longer sees cyber as a problem of technology or security, but also as a key element of sustainability of companies, permeating the very manner of conducting business, and one that is of key significance for the strengthening and further development of a stable economy.

Apart from Britain, many other countries have also decided to help the development of the industries related to cyber security, through cooperation with the private and the academic sector. Israel has, aiming to become the world leader in the area of cyber security[169], set out within the National Cyber Initiative, transformed the desert area Be'er Sheeva into a state-of-the-art research, education and development centre through the Cyber Spark industrial initiative[170] - the perennial strategic venture of a public-private partnership between the Government of Israel, the renowned Ben Gurion University and large domestic and foreign ICT companies. This resulted in research and development centres, centres of excellence, state-of-the-art university programmes and laboratories, technological incubators and innovative centres.

Germany developed the Software Cluster[171] at the South-East of the country which represents a dominant network of companies, centres of excellence and research and development institutions in the area of business software development. Similarly, the Netherlands

---

167 UK Cyber Security: The role of insurance in managing and mitigating the risk. March 2015. HM Government and MARSH.

168 The UK Cyber Security Strategy 2011-2016. Annual Report. April 2016. Cabinet Office. Crown Copyright 2016.

169 Israel Leads the World in Protecting the Web. Homeland Security and Aerospace. Israel Export Institute. http://www.export.gov.il/eng/Branches/Technologies/DefenceIndustries/News/news,8454/.

170 CyberSpark. Israeli Cyber Innovation Arena. http://www.cyberspark.org.il/.

171 Software-Cluster. http://www.software-cluster.com/en/.

developed the Security Delta[172] cluster in the Hague, and, just like Germany and other European countries, it used the regional subsidies provided by the European Union. A significant source of financing, however, came from the private sector, as well as from EU funds for the development of research.[173]

In most of these initiatives, public-private partnership plays the key role: the state sets the strategic framework and offers administrative and partial financial aid (including through international projects as well), the private sector provides the cutting-edge technology and investments, the expert communities provide the knowledge and the contacts, and the universities the existing base of knowledge and the potential for the development of research and engagement of the young through business incubators and star-up projects. This kind of an approach is also an opportunity for Serbia to use the existing potentials for the development of solutions for cyber security (primarily software and services) and raise its competitiveness in this perspective branch of export – primarily in the region where the neighbouring countries, such as Romania and Bulgaria are already well positioned.

172 The Hague Security Delta. https://www.thehaguesecuritydelta.com/.

173 V. Radunović & D. Rüfenacht. Cybersecurity Competence Building Trends. Research Report. February 2016. DiploFoundation. https://issuu.com/diplo/docs/cybersecurity_full_report.

VIII RELATED LAWS AND STRATEGIC DOCUMENTS

In order to achieve harmonisation across the entire national normative framework, it is necessary to regularly update existing regulations in accordance with newly adopted legislation. In that sense, upon adoption of the Law on Information Security, it is necessary to consider the amendments and addenda or possible adoptions of the new versions of a certain number of laws and regulations, which are primarily and directly related to:

The **Law on Personal Data Protection** ("Official Gazette RS" no. 97/2008, 104/2009 – other law, 68/2012 – decision of CC and 107/2012) is a regulation, the revision of which, in regard to information security, is highly necessary regardless of the adoption of the Law on Information Security. Nevertheless, following the entry into force of the Law on Information Security, it is of the utmost necessity to revise the provisions on particularly sensitive data, given that the systems processing these belong to ICT systems of special importance. Moreover, the Law on Personal Data Protection prescribes the obligation of undertaking technical measures for protecting data, but these measures have not been more closely regulated. This is why the Law on Personal Data Protection should align these measures with the measures for the protection of ICT systems as stated in the Law on Information Security.

The **Criminal Code** ("Official Gazette RS" no. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009, 121/2012, 104/2013 and 108/2014) in its articles 298-304a specifies the criminal acts against security of computer data. At the very least, these criminal acts should be supplemented with qualified forms, in cases when the subjects of the criminal acts are ICT systems and ICT systems of special importance.

The **Law on Organization and Competences of Government Authorities in Combating Cyber-Crime** ("Official Gazette RS" no.61/2005 and 104/2009) has, for the first time in Serbia, established competent authorities for combating cybercrime. The competence of these authorities should be expanded in line with the provisions of the Law on Information Security.

The **Data Secrecy Law** ("Official Gazette RS" no. 104/2009) governs the unique system of identifying and protecting secret data. This law is of particular importance, given that the Law on Information Security, in several places, prescribes special procedures and measures of protection which pertain to secret data, but at no point does it define them, referring instead to this Law.

The **Law on Electronic Signature** ("Official Gazette", br. 135/2004) which governs the rights, obligations and responsibilities relating to electronic certificates and which is applied in the work of state authorities and the process of submission and preparation of decisions of state authorities in electronic form, and the **Law on Electronic Document** ("Official Gazette", br. 51/2004) which governs the conditions and the manner of handling an electronic document in a legal transaction, administrative, court and other procedures, are regulations which represent the basis for the development of e-Government, and as such must be adapted to new challenges of information security.

The **Law on Electronic Communications** ("Official Gazette RS" no.44/2010,60/2013 – decision of the CC and 62/2014) governs the security and integrity of electronic communication networks and services by having the Operators committing to apply adequate technical and organizational measures, and especially measures for the prevention and minimisation of impacts of security incidents on users and interconnected networks, as well as measures for ensuring the continuity of operation of public communication networks and services. According to this Law, in case of an incident, the Operators are obliged to inform RATEL thereof, whereas according to the Law on Information Security, in case of an incident, the Ministry competent for the Information Security operations shall be informed.

The new **Law on General Administrative Procedure** ("Official Gazette RS" no. 104/2009) has entered into force on March 9, 2016 and is to be applied as of June 1, 2017, notwithstanding certain provisions whose application is to commence as of June 7, 2016, such as for example, Article 9, which governs the "Principle of Effectiveness and Economics of Procedures" according to which the state authorities are obliged to have insight into the data on the facts necessary for making decisions, to obtain these and process them as well. This basically means that an increase in the volume and frequency of exchange of data is expected among state authorities, which creates new, or rather, greater risks to information security.

The National Security Strategy of the Republic of Serbia, adopted as far back as 2009, represents the most important, strategic document which defines the basic security policies for the protection of national interests of Serbia. Although the tendency of a constant increase in risks from cybercrime and the jeopardising of information and telecommunication systems has been recognized by this document, as well as the need to develop strategic partnerships with the states which are the bearers of contemporary technologies, it is necessary for the new Strategy, which is expected during 2017, to pay more attention to the issue of information security, as one of the priority areas.

IX CONCLUSIONS AND RECOMMENDATIONS

Having adopted the Law on Information Security, Serbia has, undoubtedly made a first, major step to the establishment of a new umbrella mechanism for national information security. The upcoming short-term steps, in regard to the adoption of the necessary by-laws and the Strategy for the Development of Information Security, need to be approached with the aim of further constructive and efficient development and strengthening of policies and capacities in this field. This process, primarily, has to involve all relevant actors, who can, with their knowledge and experience, contribute to better quality solutions, but who can also provide the technical support in case of an incident. On the other hand, their inclusion in the decision-making process ensures support of a wider scope of actors for the policies adopted. Without a strong public-private partnership there is no efficient development of sustainable policies nor efficient mechanisms for information security in Serbia.

In the process of further regulating the field of information security through the adoption of bylaws and development of a strategy, apart from including various actors, existing principles and recommendations of international authorities should be relied upon. Bearing in mind that, with the existence of specific national strategic goals, the majority of national information security strategies, in their basic elements, do not differ significantly, the same should be included in the Strategy for the Development of Information Security in Serbia, whereas the specific elements will depend both on the strategic orientation of the country in terms of what elements of information security areas are a priority, as well as on the assessment of specific risks and the possibilities with which Serbia is faced and which it has access to, respectively.

In line with the strategic orientation of the country, the need of complying with the latest normative trends in the European Union and other international organizations and bodies which Serbia takes part in and cooperates with should be kept in mind, such as the Organisation for Security and Cooperation in Europe, the United Nations and NATO. In that sense, the development of policies in the field of information, i.e. cyber security needs to be continuously monitored at the international level, while considering necessary amendments and addenda of existing national legislation, as well as the adoption of new regulations if needed in accordingly.

Efforts made within further development of normative and operational elements, mechanisms and capacities in the field of information security in Serbia should strategically

include short-term, medium-term and long-term measures and in that sense, the following recommendations have been formed.

Short-term

- When adopting the Rules of Procedure of the Body for the Coordination of Information Security, clearly define the procedure for the formation of expert working groups, considering the possibility of establishing a permanent, expert, multistakeholder group, which would serve as a forum for the exchange of knowledge, experience and information, that is, for linking relevant actors from the public and private sector, but also from the academic community and the civil sector, in the form of public-private partnership.

- Develop more efficient mechanisms of informing all stakeholders of the possibilities which various international organisations provide for financing projects in the field of information security and support local and international cooperation for the purpose of using such potentials.

- Introduce ICT modules, in the shortest period of time possible, into elementary education, for the purpose of improving ICT literacy of future generations, as well as forming a basis creating a market of IT experts.

Medium-term

- In case of possible amendments and addenda to the Law on Information Security, define more clearly the position and role of the Body for the Coordination of Information Security, so as to enable more efficient functioning of the Coordination Body itself and to create a legal framework for the development of cooperation with other actors in the future, within the concept of public=private partnership.

- Develop programmes for continuous capacity building for all levels of state administration and decision-makers, in line with their authorisations and activities. The programmes should encompass political (awareness of the significance, risks and possibilities that the issue of information security carries, compliance with the principles, standards and legislation of the European Union and other international actors) as well as technical issues, in regard to the development of more efficient, operational mechanisms, and the inclusion of other actors in all segments. All state administration employees should have basic knowledge of this field, whereas some categories of the state administration should undergo a special training. For example, in Serbia, a common problem in the implementation of the adopted strategies and plans is the resistance of the middle management in the competent institutions, which therefore needs to understand the basic concepts and information security principles. In that sense, for example, NATO CCD CoE even recommends the creation of cross-sector coordination groups of middle management, for the purpose of more efficient alignment of

various requests of public authorities and better understanding of the technical requirements stemming from the expert community and the users. Through the aforementioned trainings, the representatives of middle management will be able to more easily "translate" such technical requirements into the "political language" susceptible to decision-makers.

- Step up systematic cooperation and coordination with partners in the field of cyber policies, through capacity building of sectors for international relations in institutions, especially by creating sectors for cyber diplomacy at the Ministry of Foreign Affairs and coordination of participation of state representatives, as well as representatives of the private and civil sector in key international events in this field.

- Develop multidisciplinary undergraduate and post-graduate programmes at universities, which link technical knowledge and knowledge at the policy level in the field of information security, so as to overcome the gap between these two communities, whose cooperation is crucial for future development of information security.

Long-term

- Bearing in mind the scope of work, the fact that the issues of information security refer to various aspects of the functioning of the state (security, economy, education, services, citizens' rights and the like) and the number of institutions expected to contribute to the construction of a system in this field, the formation of a separate governmental body for information security needs to be considered, which would have a key role in the vertical (through levels of the state administration) and the horizontal (through all sectors and actors) coordination and formulation of policies in this area, maintenance of a permanent dialogue and advocacy for the issues of information security to be set and to remain at the top of the political agenda.

- In cooperation with existing universities and expert communities, as well as interested domestic and international companies, establish networks of research and development centres, centres of excellence, laboratories, technological incubators and innovative centres, so as to ensure conditions for domestic IT experts to use the acquired knowledge and develop ideas in the area of information security in Serbia. This will, simultaneously, contribute to the development of the economy in this field and even further.