Guide through Information Security
in the Republic of Serbia 2.0

GUIDE
THROUGH INFORMATION SECURITY IN THE REPUBLIC OF SERBIA 2.0

Author:
Irina Rizmal

Title:
Guide through information security in the Republic of Serbia 2.0

Publishers:
OSCE Mission to Serbia, Belgrade
Unicom Telecom, Belgrade
IBM, Belgrade
Juniper, Belgrade

Design and prepress:
comma | communications design

Print:
Grid studio, Belgrade, 2018

Copies:
200

Belgrade, 2018

ISBN 978-86-6383-078-3

Content

Content

Content

LIST OF ACRONYMS

CBMs	confidence building measures
CERT/CIRT	Computer Emergency Response Team/Computer Incident Response Team
nCERT	national Computer Emergency Response Team
govCERT	government Computer Emergency Response Team
CFSP	Common Foreign and Security Policy (*European Union*)
CoE	Council of Europe
CI	critical infrastructure
CII	critical information infrastructure
CIWIN	Critical Infrastructure Warning Information Network (*European Union*)
CSDP	Common Security and Defence Policy (*European Union*)
ECSO	European Cyber Security Organisation

LIST OF ACRONYMS

EDA	European Defence Agency
EEAS	European Union External Action Service
EFSI	European Fund for Strategic Investments
ENISA	European Union Agency for Network and Information Security
ESOs	European Standardisation Organisations
EU	European Union
GGE	Group of Governmental Experts (*United Nations*)
ICT	information and communication technology
IMPACT	International Multilateral Partnership Against Cyber Threats
IPA	Instrument for Pre-Accession (*European Union*)
IPAP	Individual Partnership Action Plan (*NATO, agreed with*)
ISAC	Information Sharing and Analysis Centres

LIST OF ACRONYMS

ISP	internet service provider
ITU	International Telecommunications Union
NATO	North Atlantic Treaty Organization
NICP	NATO Industry Cyber Partnership
NIS	network and information security
OSCE	Organization for Security and Co-operation in Europe
PARP	Planning and Review Process (*NATO*)
PfP	Partnership for Peace (*NATO, programme of*)
PPP	public-private partnership
RATEL	Regulatory Agency for Electronic Communications and Postal Services of the Republic of Serbia

LIST OF ACRONYMS

SPS	Science for Peace (*NATO, programme of*)
UN	United Nations
UNDP	United Nations Development Programme
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs

FOREWORD

I consider it a great priviledge to have the opportunity to write these few lines of the foreword to the „Guide through Information Security in the Republic of Serbia 2.0“.

Among relevant actors in the field of cyber security in the Republic of Serbia, from the public to the private sector, I believe there are almost none who have not read the first edition of the Guide and whom it did not help and widen their views of this complex and multidisciplinary field.

Satisfied with the pace of development of cyber security in our country or not, it is a fact that significant steps have been made since the time of writing of the first edition of the Guide. Precisely for this reason we have eagerly awaited the new edition that is now before us.

The greatest quality of the first edition of the Guide were its systematic approach, scope and actuality of the analysis it provided. The author has managed to – with the same level of quality – research, analyse and provide a comprehensive overview of the current state and further opportunities for developing cyber security, making thus a great contribution to all of us, not only as individuas, but to our society as a whole.

Public-private partnership is one of the imperatives in developing cyber security. In this sense, it is an even greater pleasure that our company Unicom Telecom, together with our partners – IBM and Juniper Networks – had the opportunity to contribute to the preparation and print of this Guide.

Aleksandar Đorđević

CEO

Unicom Telecom

INTRODUCTION

Welcome to the Guide through Information Security in the Republic of Serbia 2.0.

The guiding idea behind this publication is to provide a comprehensive overview of the state of affairs of cyber security in the Republic of Serbia, focusing on the normative and strategic framework established thus far. This is analysed in relation to obligations and expectations the country is faced with given its membership in, and cooperation with, different international and regional regimes, organisations, initiatives and mechanisms. In order not to pose authoritatively, the study also provides information, facts and hints at where and how the Republic of Serbia can seek advice, partners and general support for establishing and strengthening its overall national cyber security framework, working thus at the same time towards fulfilling its obligations to international partners.

The Guide through Information Security in the Republic of Serbia 2.0 has its roots in an earlier edition, published by the OSCE Mission to Serbia, under the title *Guide through Information Security in the Republic of Serbia*. The first edition of the Guide had its reprint published by a private company, Saga New Frontier Group, after being recognised as a publication providing practical and constructive guidelines for further developments in this sector, through a multidisciplinary and holistic approach, aiming to unite and find a common ground between all relevant actors in the country - from public to private, from strategic to operational sectors.[1] The study in front of you therefore poses as an updated and revised version of the previous publication, compiled with the idea of continued development of comprehensive reference documents for all stakeholders engaged in the cyber security framework in the Republic of Serbia. It is important to note that many of the arguments, analyses, conclusions, and recommendations put forward in this Guide are a result of the work of an informal public-private partnership framework referred to as the '*Petnica Group*', as is explained in the following chapters. This publication, as well as its previous version, should therefore be seen as a by-product of joint efforts aimed at establishing an operational public-private partnership framework in the country, and the author would use this opportunity to thank all members of this Group.

The study was compiled between February and August 2018, mainly through desk research of publicly available literature, materials and official documents dealing with and regulating this field.

1 Foreword to the second edition of the Guide through Information Security in the Republic of Serbia. 2017. Saga New Frontier Group.

Given that the Republic of Serbia has thus far already established the basic tenets of a national cyber security framework, including normative and institutional mechanisms as well as semi-formal public-private cooperation channels, this Guide aims to commend the accomplishments of such development, but also point to certain discrepancies and deficiencies flagged in the process of implementation in practice. It is intended to pose as a comprehensive, informative tool for all stakeholders that have a direct or indirect interest in cyber security in the Republic of Serbia and a modest contribution to efforts aimed at developing a comprehensive national cyber security framework.

The first chapter, *International obligations*, analyses the principles, standards and norms the Republic of Serbia has signed up for through its strategic choice of membership in, and cooperation with, international and regional regimes, organisations, initiatives and mechanisms, including the European Union, North Atlantic Treaty Organization, Organization for Security and Cooperation in Europe, and the United Nations. In the second chapter, *National framework*, the normative and institutional mechanisms established in the field of cyber security in the Republic of Serbia are analysed, including the Law on Information Security, its complementary bylaws, as well as amendments, and the Strategy for the Development of Information Security and accompanying Action Plan for its implementation. Existing cooperation mechanisms are also discussed, focusing mainly on initiatives of public-private partnership, highlighting the benefits such cooperation can bring for overall national security in the cyber sphere. The third chapter, *Opportunities*, maps the possibilities made available to Serbia through its engagement at the international level, in terms of program-related financial resources and capacity-building programs provided by different international partners in the field of cyber security. The final chapter *Conclusions and recommendations* lists general impressions gathered through the above mentioned analysis pertaining to the state of affairs of cyber security in the Republic of Serbia, expectations and opportunities, and lists short, medium and long term conclusions based on, and tailor-made to, these local circumstances.

Special gratitude needs to be expressed to Unicom Telecom for recognising the benefits of this Guide for developing an information security framework in the Republic of Serbia and supporting the publication of its second, updated and reviewed edition.

NB: A special note pertains to the terminology used in the study, namely, to 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 at the international level too[2], without attaching primacy to either term, "information security" is, for the purpose of this study, used in relation to the national normative and strategic framework in the Republic of Serbia, since the term is, as such, employed in official documents. In parallel, "cyber security" is used in its core format, as found in official documents of international and regional regimes, organisations, initiatives and mechanisms.

2 In expert circles, the term "information security" is commonly understood as referring to the protection of confidentiality, integrity and availability of information, while the term "cyber security" includes both the protection of networks and infrastructure, as well as the protection of users. In practice, 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, for example, the countries of the Shanghai Cooperation Organization generally employ the term "information security" as a broader concept that additionally includes threats in the form of information war and propaganda.

INTERNATIONAL OBLIGATIONS

Given the Republic of Serbia's aspiration and officially proclaimed national strategic goal of becoming a European Union Member State, the country's primary reference for 'all things cyber' should be placed within the EU framework. In this sense, the country should closely monitor developments in the Union when it comes to matters of cyber security in different shapes and forms in order to align itself as much as possible with EU policies and principles. Given that the Republic of Serbia is still in a relatively early stage of developing its comprehensive national framework regulating cyber security, it makes it all the easier to introduce practices based on EU standards from the very outset, rather than having to go through painful processes of changing established practice in order to align with the Union's approach.

In terms of other international obligations, the Republic of Serbia, despite acting from a position of a militarily neutral country and one not aspiring to become a member, nevertheless maintains a high level of cooperation with the North Atlantic Treaty Organisation (NATO). Such cooperation is practiced through membership in the Partnership for Peace framework, and the accompanying Planning and Review Process (PARP). Additionally, in 2015, the Republic of Serbia agreed an Individual Partnership Action Plan (IPAP) with NATO, establishing thus the highest level of cooperation a country not aspiring to become a member can have with the Alliance. Within this agreement, among other things, Serbia has also obliged itself to take certain steps in the field of cyber security.

Finally, in order to step up on the international stage and carve a position for itself at international negotiating tables dealing with matters of cyber security, the Republic of Serbia needs to monitor, implement and practice different principles promoted and adopted by international organisations it is a member of. Primarily, these refer to measures suggested and promoted by the Organization for Security and Co-operation in Europe (OSCE), as well as principles and conclusions arrived at within the United Nations (UN). Although voluntary in their essence, these measures provide initial guidelines based on facts and practical experiences for establishing and developing regulatory and operational frameworks for raising national cyber security levels and developing international cooperation in this field.

European Union

As a multi-national ecosystem, the European Union can be said to have the most developed international framework regulating cyber security matters. As a genuine portrayal of the essence of the nature of cyber security, the EU cyber security framework approaches this issue from a number of different lenses – security, economic and political – addressing a myriad of challenges and opportunities cyber as a field implies and opens. These range from questions of resilience and critical information infrastructure protection across the Union and within its Member States, to the Digital Single Market and security standards in ICT products based on 'security by design' principles, to foreign policy and cyber diplomacy. Through the evolution of cyber security policies in the Union, synergies between lenses of security, economy and policy arise as cross-cutting issues emerge, resulting in comprehensive policies establishing umbrella governance frameworks. To date, the majority of cyber security efforts within the Union have been supported by the European Union Agency for Network and Information Security (ENISA), whose role, among others, is to work together with EU Members States and the private sector to deliver advice and solutions, including cyber exercises; support development of national cyber security strategies, cooperation and capacity building of Computer Emergency Response Teams (CERTs); and identify the cyber threat landscape[3]. As discussed further in this chapter, pending developments see a proposal for widening ENISA's mandate, establishing the body as a European Cyber security Agency.

Security lens

With security posing as a key precondition for any additional developments in cyberspace, the European Union adopted the **Cyber Security Strategy of the European Union**[4] in 2013, as the first umbrella document of the European Commission to assume a comprehensive strategic approach to cyber security across the Union. As its first strategic priority – 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 the Republic of Serbia is to align itself with in the process of 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 states and the private sector. Priorities set by this Strategy additionally include capacity building, international dialogue on cyberspace, as well as implementation of fundamental principles of the EU, such as openness and freedom, in cyberspace.

---

3 ENISA website. https://www.enisa.europa.eu/about-enisa.

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

Moving onto more specific issues, matters pertaining to critical infrastructure in the area of information and communication technologies build 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**[5]. According to this Directive, 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. The 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, call for application of the same approach in other sectors too, specifically, information and communication technologies[6].

In March 2009, on the basis of the Communication on Critical Information Infrastructure Protection, the **European Public-Private Partnership for Resilience (EP3R)**[7] 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 existing models of existing national public-private mechanisms, encourage information sharing and stock-taking of good practice; enable discussion on priorities, objectives and measures of public policies in this field; and identify the basic preconditions for security and resilience in Europe. This endeavour was completed in 2013 and shut down after four years of operations. In 2016, a more ambitious and comprehensive form of public-private partnership in cyber security was established, as will be discussed further on.

In the meantime, in 2013, the **Critical Infrastructure Warning Information Network (CIWIN)**[8] was set up as a pilot project - 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 eleven critical sectors. Despite primarily focusing on EU Member States, the CIWIN platform also allows access to governmental authorities, organizations and experts from third countries having formal cooperation with the EU on activities pertaining to the protection of critical infrastructure.

The **European Agenda on Security**[9], adopted in 2015, lists cybercrime as one of its three core priorities requiring immediate action, alongside terrorism and organised crime. In

---

5 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 345/75.

6 The European Commission draws up the guidelines for identification of European critical infrastructure in the Member States, but this document is classified.

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

8 Critical Infrastructure Warning Information System (CIWIN). European Commission. https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en.

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

this sense, cyber security is defined as the 'first line of defence' against cybercrime, and swift adoption of a comprehensive framework governing network and information security across the Union is called for.

This took place in 2016, with the adoption of the **Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)**[10], following three years of complicated negotiations between the Commission, the European Parliament and the Council of Europe. The NIS Directive calls on all Member States to prescribe the basic standards relevant to the security of national network and information systems that are to be defined by the competent state authority and establish functional Computer Emergency Response Teams (CERTs), along with adopting national strategies and cooperation plans in this field. According to the 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 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 existing industry practices, and one that Serbia is still struggling to introduce as a baseline standard for any planned activities and actions. The need for *standardisation* is underlined as well, in order to ensure common security throughout the EU, proposing the development of harmonized standards. Providing a step-by-step detailed list of elements that national cyber security frameworks should consist of, the NIS Directive poses as a baseline checklist for any country aiming to develop a sound national approach in this field, not to mention its importance of acting as an integral guideline for aspiring EU Member States, as is the Republic of Serbia. To this end, the current Law on Information Security, and its complementary bylaws, are expected to be updated and revised to be fully aligned with the Directive's provisions.

10 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. Official Journal of the European Union. L 194/1.

According to the NIS Directive, support to strategic cooperation among Member States is provided by the **Cooperation Group**[11] that is made up of representatives of Member States, the Commission and ENISA. Eighteen 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 – which is an opportunity the Republic of Serbia should explore. Otherwise, according to the Commission implementing decision on the Cooperation Group's procedural arrangement, representatives of acceding countries shall automatically be invited to attend the Group's meetings following the signing of the Treaty of accession. The Chair may also invite representatives of relevant stakeholders or experts to participate in a meeting or in a particular part of a meeting of the Group, on his/her own initiative or at the request of a member of the Group.[12]

In terms of critical information infrastructure, the NIS Directive prescribed that 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 and III contain 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, as they are generally referred to in the normative framework of the Republic of Serbia). According to the list of services, this group is in fact presented as equivalent to operators of critical infrastructure, encompassing the:

- Energy sector (electricity, oil and gas);
- Transport sector (air, rail, water and road transport);
- Banking sector;
- Financial market infrastructures;
- Health sector (healthcare settings including hospitals and private clinics);
- Drinking water supply and distribution; and
- Digital infrastructure (IXPs, DNS service providers and TLD name registries). (Annex II)

---

11 According to Article 11 of the NIS Directive, the Cooperation Group is tasked with providing strategic guidance for the activities of the CSIRTs network and discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice.

12 Commission implementing decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. L 28/73.

- Online marketplace;
- Online search engine; and
- Cloud computing service. (Annex III)

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 as well as the methodology for identification and classification of importance of the said service providers. These are all submitted to the European Commission.

Further specific principles prescribed by the NIS Directive pertain to developing additional rules and/or guidance on cyber risk preparedness for critical sectors. To this end, Member States are advised to develop a national strategy that encompasses all relevant dimensions of society and economy, and not only the sectors and digital services covered respectively in the mentioned Annexes II and III the NIS Directive. This would imply adopting legislation that provides a higher level of security of network and information systems, encompassing sectors other than solely those listed in the Directive's Annexes. A hint at what these systems may be is provided in the Commission's Communication on **Making the Most of NIS**[13], listing public administration systems and services, the postal sector, the food sector, chemical and nuclear industry, the environmental sector and civil protection. Such lists should be considered as the guiding principles in Serbia's efforts to map its critical information infrastructure. As part of the latest steps taken towards establishing an EU resilience system in cyberspace, 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 developing specific rules and/or guidelines on cyber risk-preparedness for such critical sectors.

Building upon the tenets set by the NIS Directive, the Commission further prescribes additional procedural developments aimed at standardisation, enabling a more coordinated response among Member States and by the Union as a whole[14]. To this end, the Commission suggests that Member States should, supported by ENISA, cooperate in developing and adopting a common taxonomy and template for situational reports to describe the technical causes and impacts of cyber security incidents to further enhance their **technical and operational cooperation during crises**, taking into account the work of the mentioned Cooperation Group on incident notification guidelines and, in particular, aspects related to the format of national notifications. Such procedural developments would enable a more coordinated and ultimately a more efficient way of responding to cyber incidents and threats and challenges stemming from cyberspace through the introduction of unified

13 Annex to the Communication from the Commission to the European Parliament and the Council. Making the Most of NIS – Towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. 13.9.2017. COM(2017) 476 final ANNEX 1

14 Commission recommendation of 13.9.2017. on Coordinated Response to Large Scale Cyber security Incidents and Crises.

incident notifications as part of crisis communication and management. Given the Serbian Government's efforts in developing and completing the national normative cyber security framework, these expected procedures should be taken into account when updating the adopted Regulation on the procedure for data submission, lists, types and importance of incidents and importance of incidents and procedures of notification on incidents in information-communication systems of special importance[15] as it will contribute to both having efficient and recognised national procedures, at the same time ensuring interoperability with EU countries.

In addition, the European Defence Fund[16], envisions increased investment in cyber security, among other. Namely, the European Investment Fund is to step up its contribution to the EU security and defence agenda, including investment in issues such as dual-use technologies and cyber, along with financing of civil protection measures and biodefence infrastructure. The European Defence Fund also aims at increasing the share of cooperative defence projects in overall defence spending, as well as examining complementarity with civil use and corresponding European civil support programmes. Complementarity is, in this sense, sought mostly in relation to other EU security policies, including cyber security. Therefore, further increases in investments into cyber defence capacities of EU Member States, primarily aimed at achieving interoperability and efficiency, through complementarity and sharing of resources, can only be expected.

Finally, as part of efforts aimed at renewing the 2014 EU Cyber Defence Policy Framework, focus is placed on cyber-resilience of Common Security and Defence Policy framework missions and operations in terms of standardised procedures and technical capabilities to support both deployed civilian and military missions and operations, as well as their respective Planning and Conduct Capability structures and EEAS information technology service providers. Given that the Republic of Serbia actively takes part in a number of EU missions, this notion should be of its concern as a potential to widen the scope and nature of the country's engagement in such missions through involvement in dedicated cyber resilience teams.

In addition, with EU efforts focused on **resilience, deterrence and defence**[17], prioritising the establishment of a strategic framework for conflict prevention and stability in cyberspace in its bilateral, regional, multi-stakeholder and multilateral engagements, and given its focus prioritising the Union's neighbourhood and developing countries, the establishment of a EU Cyber Capacity Building Network is foreseen. The Network will bring together the European External Action Service (EEAS), Member States' cyber authorities, EU agencies, Commission services, academia and civil society. Together, these actors would

15 Regulation on the procedure for data submission, lists, types and importance of incidents and importance of incidents and procedures of notification on incidents in information-communication systems of special importance. *"Official Gazette of the Republic of Serbia"* no.94. November 24, 2016.

16 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Launching the European Defence Fund. 7.6.2017. European Commission. COM(2017) 295 final.

17 Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

work on developing EU Cyber Capacity Building guidelines to help offer better political guidance and prioritisation of EU efforts in assisting third countries. To this end, a new cyber platform to coordinate education, training, evaluation and exercises (ETEE) in the field of cyber security/defence across Europe will be launched in September 2018.[18] The European Security and Defence College (ESDC) will be tasked with managing the platform, focused on education, training, evaluation and exercises (ETEE) in the field of cyber security/defence. The full operational capability of the platform is planned to be announced in April 2019.

Latest developments see cyber matters included also in roadmaps for developing **Permanent Structured Cooperation (PESCO)[19]**. PESCO aims at developing closer cooperation between EU Member States in the areas of security and defense. It envisions development of joint defence capabilities, investment in shared projects and enhancement of operational readiness among willing and able Member States. In early 2018, the Council adopted an initial list of seventeen projects, previously identified by the (currently) twenty-five participating Member States. Among these, two projects directly address matters of cyber security and defence. Namely, projects pertaining to developing a cyber threats and incident response information sharing platform, as well as cyber rapid response teams and mutual assistance in cyber security, are to be developed under PESCO.[20]

Serving as a benchmark for completion of the priorities set out in by and for PESCO, and the European Defence Fund, the European Defence Agency (EDA) adopted in June 2018 a Capability Development Plan and approved the associated EU Capability Development Priorities as a key reference for Member States' and EU's capability development initiatives.[21] Covering issues that include matters such as ground combat capabilities, air superiority and naval manoeuvrability, the 2018 EU Capability Development Priorities place enabling capabilities for cyber responsive operations at the very top of planned lines of action.

***

18 New EU cyber platform to boost cyber security capabilities across Europe. 14. 2. 2018. European Union External Action Service.

19 Council Decision establishing Permanent Structured Cooperation (PESCO) and determining the list of Participating Member States. 8.12.2017. Council of the European Union. CORLX 548. CFSP/PESC 1063. CSDP/PSDC 667. FIN 752.

20 Council Decision of 6 March 2018 establishing the list of projects to be developed under PESCO. Council of the European Union. PRESS.

21 New 2018 EU Capability Development Priorities approved. 28 June 2018. European Defence Agency.

Cross-sector cooperation

Within further efforts aimed at establishing a common and comprehensive framework for cyber security across the European Union, in May 2018, an additional step was made to bring civil-military cooperation closer, establishing synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector, as called for by the 2014 Cyber Defence Policy Framework. To this end, ENISA, EDA, the European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) signed a Memorandum of Understanding (MoU) to establish a cooperation framework between their organisations.[22]

The MoU aims at leveraging synergies between the four organisations, promoting cooperation on cyber security and cyber defence between these EU agencies. More specifically, it focuses on five areas of cooperation, namely, exchange of information, education and training, cyber exercises, technical cooperation, and strategic and administrative matters. It also allows for cooperation in other areas identified as mutually important by the four organisations. Although mainly working independently on these matters, the step marks an official move towards adopting a wider, cross-sector approach, combining operations of agencies that focus on security, defence and crime detection and prevention efforts, thus widening further the Union's approach to cyber security considerations and actions. Including the cybercrime agency (EC3) in an official cooperation framework related mostly to cyber security is an important shift from the current practice of strict delineation between cybercrime and cyber security, when it comes to jurisdictions of EU institutions and agencies.

Economic lens

Being, above all, an economic Union, the EU has fairly early recognised the potential to be unlocked by both developing a cyber security industry and implementing cyber resilience to protect other economic spheres and activities. To this end, a number of steps have thus far been taken aimed at introducing measures based upon which the Digital Market can evolve and strengthen. Most notably, these include a number of activities setting the ground for Union-wide standard development.

In this sense, the **Digital Single Market Strategy for Europe**[23] clearly recognised the importance of cyber security for the functioning of the digital market. The Strategy highlights the need to define missing technological standards supporting the development of the digital market and services sector – including cyber security-specific standards. The Roadmap for completing the Digital Single Market included in this document envisages

22 Four EU cyber security organisations enhance cooperation. May 23, 2018. European Union Agency for Network and Information Security.

23 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 May 2015. European Commission. COM(2015) 192 final.

adoption of a Priority ICT Standards Plan, as well as establishment of a Cyber security contractual Public-Private Partnership, which took place in mid-2016.

The **contractual Public-Private Partnership for cyber security industrial research and innovation (cPPP)**[24] managed to attract as much as 1.8 billion Euros of investment by 2020, triggering efforts aimed at further developing this concept. The Partnership is set up as a contractual arrangement for public-private cyber security industrial research and innovation between the European Union, represented by the Commission on the one side, and the **European Cyber Security Organisation (ECSO)**[25] on the other. Initially intended to remain in force until December 31, 2020, the cPPP is, among other, to coordinate the partnership implementation with EU Member States, Regions, other national public administrations participating in the partnership, third countries and other Horizon 2020 instruments and sectorial PPPs, as well as cooperating with third countries. Efforts are aimed at harmonising approaches in the cyber security market, in particular fostering the development and use of international standards wherever possible, as well as attracting the stakeholder community investment for projects implementing the research and innovation agenda under the Horizon 2020 Framework Programme.[26]

In light of this development, and as part of further efforts to this end, an initiative to establish a network of cyber security competence centres, with a **European Cyber security Research and Innovation Centre** at its heart, has been communicated to the European Parliament and the Council in September 2017.[27] The network would consist of existing and future cyber security centres established in Member States, including public research centres and laboratories. In its efforts to spark official establishment of the network, the Commission will propose a pilot phase under the Horizon 2020 to link national centres, complementing thus the continued development of the public-private partnership on cyber security. The Centre is seen as a potential focal point for multinational project management working on a myriad of issues including the development of next-generation digital technologies, High Performance Computing infrastructure and cyber security certification, among others.

When it comes to **developing a standardized approach**, the **CEN-CENELEC Focus Group on Cyber Security**[28] (previously known as the Coordination Group for Cyber Security), led

24 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.

25 European Cyber Security Organisation (ECSO). http://www.ecs-org.eu/membership.

26 Annex: Contractual Arrangement setting up a Public-Private Partnership in the area of Cyber security Industrial Research and Innovation between the European Union and the European Cyber security Organisation to the Commission Decision on the signing of a contractual arrangement setting up a public-private partnership in the area of cyber security industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. 2016. European Commission.

27 Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

28 CEN-CENELEC Focus Group on Cyber security. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cyber security.aspx.

by the European Agencies for standardisation CEN[29] and CENELEC[30], 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 the development of a regulatory framework that would allow thorough implementation thereof.

Furthermore, the **Governance Framework for European Standardisation**[31], of the European Union Agency for Network and Information Security (ENISA), in addition to recommendations for standardisation, also lists the relevant actors to be included in the process. Alongside industry, state administration, national bodies for standardisation, the users' community and academia, the Governance Framework also lists transnational European Standardisation Organizations (ESOs) as recognized by the European Commission. ESOs are seen as key actors for enabling 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 thirty-three European countries.

The mentioned **ICT Standardisation Priorities Plan**[32], adopted in April 2016, lists among five priority areas (such as 5G communications and big data technologies) cyber security, as an independent field and one of the "essential technology building blocks" for establishing 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 partnership (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, and accompanying guidelines for revision for supervisory authorities and regulatory bodies.

Latest developments in the field of standardisation see proposals for attaining the goals of a Single Cyber security Market through the introduction of an **EU-wide certification scheme**[33], based on a 'security by design' principle. This is a strategic decision already envisioned by a number of EU Member States, calling upon efforts to this end within their national cyber security strategies. According to this proposal, a **European Cyber security Certification Group** is to be established as an advisory body for the Commission on issues concerning cyber security certification policy and contributing to the development of draft European cyber security certification schemes. The Group is to be composed of national

29 European Committee for Standardisation.

30 European Committee for Electro-Technical Standardisation.

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

32 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.

33 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cyber security certification ("Cyber security Act"). European Commission. COM(2017) 477 final. 2017/0225 (COD).

certification supervisory authorities, represented by the heads or by other high level representatives of national certification supervisory authorities.

Factoring cyber security into trade and investment policies in the process of building the EU Single Market, the proposed cyber security certification process is envisioned as further strengthening Europe's international position, complementary with efforts towards developing high-security global standards and mutual recognition agreements.[34] With one standard applicable to all EU Member States, and recognised even beyond the Union's borders, the Republic of Serbia should undoubtedly monitor developments in this field in order to ensure any future products developed on its soil conform to such standards, especially given that developing a successful national ICT industry is proclaimed as one of the current Government's key strategic priorities.

Political lens

As a political entity, the European Union has included cyber-related matters and policies within its foreign policy and diplomacy efforts and endeavours. To this end, the **Global Strategy for the European Union's Foreign and Security Policy**[35], defines cyber security as one of the five priorities of the Union's foreign policy security issues, to be pursued within the framework of its Common Foreign and Security Policy (CFSP). The document prescribes weaving cyber issues across all policy areas, envisioning also reinforcement of cyber elements in the Union's Common Security and Defence Policy (CSDP) missions and operations.

Delving deeper into the Union's foreign policy regarding cyber security, the notion of cyber diplomacy has already been recognised as a tool for ensuring a safer global cyberspace. To this end, **Council Conclusions on Cyber Diplomacy**[36] highlight the evolving importance of building up cyber capacities of third countries as strategic building blocks, encouraging the EU and its Member States to promote sustainable cyber capacity development and streamline and prioritise funding, including by making full use of relevant EU external financial instruments and programmes. The document also calls for a new EU Cyber security Strategy to include the notion of supporting the creation of relevant national policies, strategies and institutions in third countries as part of the Union's foreign policy efforts in this field. A cyber security-focused foreign policy is thus seen as a building block contributing to developing resilient systems and mitigating cyber risks for the Union itself.

Completing the foreign policy cycle in cyberspace, the Union also developed a "cyber diplomacy toolbox", setting out specific measures under the Common Foreign and Security Policy. These include restrictive measures that can be used to strengthen the EU's response

34 Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

35 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. 2016. European External Action Service.

36 Council Conclusions on Cyber Diplomacy. 11 February 2015. Council of the European Union. 6122/15.

to activities that harm its political, security and economic interest, setting up the basis for signalling and reactive capacity development for the Union and its Member States.[37] To this end, the **Cyber Diplomacy Toolbox**[38] sets out principles based upon which the Union and its Member States are to react to malicious cyber activities, acting as a framework for a joint EU diplomatic response. The Toolbox prescribes that further work on the EU joint diplomatic response will be developed upon the following principles:

- Serve to protect the integrity and security of the EU, its Member States and their citizens;
- Take into account the broader context of the EU external relations with the State concerned;
- Provide for the attainment of the CFSP objectives as set out in the Treaty on the European Union (TEU) and the respective procedures provided for their attainment;
- Be based on a shared situational awareness agreed among the Member States and correspond to the needs of the concrete situation in hand;
- Be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity;
- Respect applicable international law and must not violate fundamental rights and freedoms.

Latest cyber security developments related to the Union's foreign policy approach have been outlined in the annual **State of the Union**[39] address. European Commission President, Jean-Claude Juncker, reaffirmed on the occasion the topic's continued presence and recognised its growing importance in the Union's policies. Namely, cyber security issues – ranging from intellectual property, cultural diversity and personal data protection, to fight against terrorist propaganda and radicalisation online, to, most notably, cyber-attacks – prominently rose as a fourth priority in the address. They took place even ahead of migration, one of the most pressing challenges the Union has recently been faced with. Calling upon figures that cite more than 4,000 ransomware attacks per day in 2016, and more than 80% of European companies experiencing at least one cyber security incident, President Juncker presented a proposal for new tools to be developed, including, specifically, the establishment of ENISA as the mentioned European Cyber security Agency.

---

37 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9,2017. JOIN(2017) 450 final.

38 Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption. 7 June 2017. Council of the European Union. 9916/17

39 President Jean-Claude Juncker's State of the Union Address 2017. 13 September 2017. European Commission. SPEECH/17/3165

Finally, the recently adopted **Strategy for the Western Balkans**[40] clearly underlines the need for operational cooperation on countering various types of organised crime to be expanded to encompass this region within the existing policy cycle. To this end, the Strategy envisions increased support to capacity building in both the field of cyber security and the fight against cybercrime, through enhanced cooperation with relevant agencies such as Europol and ENISA.

***

Sitting at the borderline between the security, economic and political aspects of cyber security concerns, the European Union's **General Data Protection Regulation (GDPR)**[41], which came fully into force on May 25, 2018, is directly applicable in all EU Member States, setting also the baseline harmonisation standard for data privacy laws across the world. Raising standards for personal data protection, GDPR also raises the bar of necessary security standards falling into the scope of cyber security frameworks, both in the public and private sector. Given the extra-territorial applicability of the Regulation, GDPR applies regardless of the country at hand or the company's location, but relates solely to personal data of data subject residing in the Union (EU citizens). Given the prescribed penalties of up to 4% of annual global turnover or 20 million Euros (whichever is greater) for organisations found in violation of the Regulation, the need for raising security standards to ensure compliance imposes itself as alarming.

One of the cornerstones of GDPR are integrity and confidentiality principles, prescribing that data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In line with this principle, both controllers and processors of data[42] are obliged to implement specific technical and organisational measures to ensure appropriate levels of security given the risks identified in each particular case. GDPR explicitly lists some of these measures, such are pseudonymisation and encryption of personal data, the ability to restore the availability and access to personal data in a timely manner in the event of an incident, as well as regularly testing, assessing and evaluating the specific measures in place.

The Regulation prescribes that controllers or processors of data which are not established in the Union shall designate a representative in the Union, established in one of the Member States where the data subjects, whose personal data is processed, are. Most relevant to

40 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A credible enlargement perspective for and enhanced EU engagement with the Western Balkans. 6.2.2018. European Commission. COM(2018) 65 final.

41 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. L 119/1.

42 For the purpose of the Regulation, a controller is understood as the entity that determines the purposes, conditions and means of the processing of personal data. The processor, on the other hand, is an entity which processes personal data on behalf of the controller.

cyber security matters, GDPR prescribes that **in the case of an identified breach, the controller shall notify the supervisory authority within 72 hours** at the latest. The notification is to describe the nature of the data breach, contact details of the data controller, likely consequences, as well as measures taken or proposed to be taken to address the breach and mitigate possible adverse effects. Based on the documentation submitted, the supervisory authority verifies compliance with the obligations prescribed.

Furthermore, the Regulation highlights that even the controllers and processors that are not subject to it may adhere to the provisions it sets out in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations. A **transfer of personal data to a third country or an international organisation** may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. The Commission will therefore assess the adequacy of the level of protection based on the rule of law, the existence and effective functioning of one or more independent supervisory authorities, as well as international commitments the third country or international organisation has entered into, in particular in relation to the protection of personal data. Once adequate levels of protection are confirmed, the Commission may decide, in the form of an implementing act, that a third country or an international organisation satisfies these, providing also a mechanism for a periodic review, at least every four years. If such a decision is lacking, data may be transferred only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and legal remedies for data subjects are available through, for example, legally binding and enforceable instruments, binding corporate rules, standard data protection clauses, an approved certification mechanism, contractual clauses or administrative arrangements.

Finally, GDPR also lays down the basis for **international cooperation** for the protection of personal data. To this end, in relation to third countries and international organisations, the Commission aims to develop international cooperation mechanisms to facilitate effective enforcement of legislation for personal data protection; provide international mutual assistance in the enforcement of legislation for the protection of personal data; engage relevant stakeholders in discussion and activities aimed at furthering international cooperation on this matter; and promote the exchange and documentation of personal data protection legislation and practice including on jurisdictional conflicts with third countries.

As in the case of the NIS Directive, the Republic of Serbia is also to align with the GDPR. Even more so given the fact that this Regulation transposes official EU boundaries. This means that the country must have adequate guarantees in place for all EU citizens whose personal data is stored and/or processed within its borders, regardless of official EU membership, in addition to seeing alignment with the Regulation as a logical step for any aspiring candidate country.

Pending developments: EU Cyber security Strategy 2.0

Latest developments in the European Union undoubtedly pose as a primarily stronger, more direct and more comprehensive approach to regulating issues of cyber security within the Union itself. To this end, proposed matters concerning the establishment of an EU Cyber security Agency as well as an EU-wide cyber security certification scheme, for the time being, are of direct concern only for EU Member States. However, it is only a matter of when these will be adopted, rather than whether they will be, and the Republic of Serbia, as a country aspiring to EU membership should take them as a baseline approach when developing its own cyber security framework. Through established and developing EU mechanisms that allow participation of third countries, Serbia should take note of principles, standards and practices in order to be able to engage in EU efforts in this field to the extent to which this is possible. On the other hand, even with direct cooperation lacking, by raising national standards and capacities in line with EU trends, the Republic of Serbia will ensure a comprehensive approach to national cyber security establishing its own capability and readiness for cooperation and engagement in EU efforts upon invitation or at the time of accession to the Union. Crucially, it will strengthen its own national cyber security posture.

To this end, an absolute prerogative, and one that the EU has been advocating for ever since more comprehensive approaches to cyber security emerged, is the principle of public-private partnerships. The European Commission recognised that governments and public authorities are reluctant to share cyber security-relevant information for fear of compromising national security or competitiveness, while private undertakings are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules. Establishing public-private partnership as a two-way street, in which both sides have their specific interests and concerns, the Commission proposes setting up of **Information Sharing and Analysis Centres (ISACs)** aimed primarily for information sharing and acting as a hub for creating the necessary trust between the public and private sector.[43]

The sheer importance attributed to matters related to cyber security in the latest developments within the Union is further demonstrated within recommendations arrived at through the consultation process with institutions and EU Member States on a "Blueprint" to provide an effective process for an operational response at Union and Member State level to a large-scale cyber incident.[44] To this end, the Commission recommended that Member States and EU institutions establish an **EU Cyber security Crisis Response Framework**[45]. Additionally, the Commission aims at investigating the possibility of establishing a **Cyber security Emergency Response Fund** based on the principles of existing

43 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. European Commission. JOIN(2017) 450 final. Previously proposed within COM(2016) 410 final.

44 Ibid.

45 Commission Recommendation of 13.9.2017. on Coordinated Response to Large Scale Cyber security Incidents and Crises. European Commission. C(2017) 6100.

EU crisis mechanisms in other policy areas. Set up like this, the envisioned Fund would enable deployment of a rapid response capability, drawing on national expertise along the lines of the EU's Civil Protection Mechanism. This would allow Member States to seek help at the EU level during or following a major incident, **provided that the Member State had put in place a prudent system of cyber security prior to the incident, including full implementation of the NIS Directive, mature risk management and supervisory frameworks at national level**.

Although these endeavours are still in a recommendation phase, if their development genuinely continues on the proposed principles of EU's Civil Protection Mechanism, the Republic of Serbia could, as a candidate country, potentially also have access to the resources made available for mitigating large-scale cyber incidents. The country has already pulled resources from the EU's Civil Protection Mechanism in 2015 to help mitigate the challenges faced in light of Europe's migrant crisis. If such reasoning is adopted, the country also needs to keep in mind the proposed conditions for access to these emergency funds to be granted – a comprehensive national approach to cyber security and full embracement, adoption and implementation of EU regulations, standards and principles, as highlighted above.

These mechanisms are proposed to be placed within the jurisdiction of an **EU Cyber security Agency**, developing on the basis of the existing European Network and Information Security Agency (ENISA). The proposal[46], put forward by the European Commission in September 2017 envisions establishing a **European Cyber security Research and Competence Centre** under the next multiannual financial framework, in addition to the development of the mentioned ISACs. In addition, the Agency would be mandated for EU policy development and implementation, capacity building, knowledge and information sharing, awareness raising, market related tasks (standardisation and cyber security certification), research and innovation, operational cooperation and crisis management.

Tasked primarily with strengthening the Union's cyber security framework, the Agency would also contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on issues related to cyber security by:

- Engaging as an observer in the organisation of international exercises, and analysing and reporting on the outcome of such exercises;
- Facilitating the exchange of best practices between the relevant international organisations;
- Providing the Commission with expertise.

46 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cyber security certification ("Cyber security Act"). European Commission. COM(2017) 477 final. 2017/0225 (COD).

In this sense, the Agency may cooperate with the competent authorities of third countries or with international organisations, with special emphasis on enabling participation of third countries that have entered into agreements with the Union to this effect. A strategy for relations with third countries or international organisations concerning matters for which the Agency is competent is to be developed to this end.

Continuing efforts aimed at fostering public-private partnerships, a **Permanent Stakeholders' Group** is also to be established, composed of recognised experts representing relevant stakeholders. These include the ICT industry, providers of electronic communications networks and services available to the public, consumer groups, academic experts in cyber security and representatives of competent authorities as well as law enforcement and data protection supervisory authorities. The Group would act as an advisory body, ensuring regular dialogue with the private sector, consumers' organisations and other relevant stakeholders, focusing on matters relevant to stakeholders and bringing them to the attention of the Agency.

The proposed Cyber security Act, aimed at strengthening ENISA's mandate and establishing an EU framework for cyber security certification, draws closer to adoption with developments seeing adoption of a general approach by the EU Telecommunications Council.[47]

Regional considerations

As part of actions focused directly on the Western Balkans region, the European Commission launched, in June 2018, the Digital Agenda for the Western Balkans.[48] Although falling primarily within the scope of the EU's Digital Agenda endeavours, aimed at supporting the transition of the region into a digital economy fostering faster economic growth, more jobs, and better services, the initiative recognises the need for effective cyber security as one of the building blocks. To this end, alongside investing in broadband connectivity, strengthening the digital economy and society and boosting research and innovation, the Commission, together with Ministers from six Western Balkan partners (Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, the former Yugoslav Republic of Macedonia and Serbia), also committed to increasing cyber security, trust and digitalisation of industry. In this sense, the EU and the Western Balkans region subscribed to a common objective of improving online trust and security, with the Digital Agenda supporting capacity building in this field.

47 Cyber security: Joint Statement by Vice-President Ansip and Commissioner Gabriel on political agreement from the Council. 8 June 2018. European Commission. STATEMENT/18/4097.

48 European Commission launches Digital Agenda for the Western Balkans. 25 June 2018. European Commission. IP/18/4242.

* This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

North Atlantic Treaty Organisation (NATO)

The North Atlantic Treaty Organisation (NATO) focuses most of its activities related to cyber on defence. The cyber sphere, declared by NATO as the fifth domain of warfare in July 2016[49], has placed matters of cyber defence as part of the Organisation's core task of collective defence, seeing allies making a **Cyber Defence Pledge**[50] that the fullest range of national cyber defence capabilities will be developed and strengthened.

This builds upon previous efforts aimed at increasing NATO cyber defence capacity, with the 2015 **Memorandum of Understanding (MoU) on Cyber Defence** to be signed between NATO and its twenty-eight Allies. The MoU sets out arrangements for the exchange of cyber defence-related information and assistance to improve cyber incident prevention, resilience and response capabilities.

Latest cyber-related developments within NATO include the establishment of a new **Cyber Operations Centre**[51] as part of an adapted structure of NATO's Command Structure. The intention behind this development is to have Allies' national cyber capabilities integrated into NATO missions and operations. As with conventional tools, national ownership is to be maintained over such capabilities, and nations will decide for themselves what kind of capabilities they are willing to use and integrate in specific NATO missions and operations.

In terms of comprehensive approaches, NATO maintains a framework for cooperation with the private sector through the **NATO Industry Cyber Partnership (NICP)**[52], established in 2014. The framework brings together NATO entities, national Computer Emergency Response Teams (nCERTs) and representatives of member states' respective industries. Efforts of the Partnership focus mainly on information and knowledge exchange, training and education, joint exercises as well as joint participation in multinational Smart Defence projects. Working together, stakeholders engaged in this partnership also aim at improving overall cyber defence in NATO's defence supply chain.

In terms of cooperation with third countries, the Alliance concludes specific partnership action plans. In this sense, in 2014, the Republic of Serbia agreed an **Individual Partnership Action Plan (IPAP)**[53], as the highest form of cooperation a country not aiming for full

---

49 Warsaw Summit Communique issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. 9.7.2016. North Atlantic Treaty Organisation. https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf. The inclusion of the cyber domain as a fifth domain of warfare means that cyber attacks now fall within the jurisdiction of Article 5 of collective defence principles.

50 Cyber Defence Pledge. 8.7.2016. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

51 Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers. 8.11.2017. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/opinions_148417.htm.

52 NATO Industry Cyber Partnership. http://www.nicp.nato.int/.

53 Individual Partnership Action Plan (IPAP) between the Republic of Serbia and the North Atlantic Treaty Organisation (NATO). 2014. Ministry of Foreign Affairs of the Republic of Serbia.

membership can establish with NATO. The document, covering the period 2015-2016, included cyber-related aspects of cooperation within Chapter 1, Foreign and Security Policy, Section 1.2.3. *Emerging Security Challenges: Fight Against Terrorism, Arms Control and Cyber-Defence*. Within it, activities aimed at enhancing capabilities for protecting critical communication and information systems against cyber-attacks as future strategic goals were envisioned. In this regard, the plan was to establish mechanisms and structures of coordination at governmental level for cyber defence. In addition, this IPAP also referred to defending against cyber-attacks in Chapter 4, Protection of Classified Information, within Goal 3: *Enhance capabilities for protecting critical communication and information systems against cyber-attacks*. Activities needed for the fulfilment of this goal correspond to those planned within the previously mentioned chapter.

The NATO Partnerships and Cooperative Security Committee (PCSC) adopted on September 26, 2016 a report on IPAP implementation which concludes that out of a total of 215 activities as many as 134 activities (62%) were carried out, 75 (35 %) have been partly implemented within the planned period, while only 6 (3%) have not been implemented at all. Implementation of this IPAP has been extended over the course of 2017. A succeeding IPAP, which is to include the period 2018-2019, is currently under preparation according to the Ministry of Defence.[54]

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 – it is *agreed* between parties without any official *signatory process* - the mere fact that the activities, i.e. areas of cooperation are proposed by the partner state indicates that there is a certain level of intention to carry these out. The contrary would create an impression of a lack of responsibility and/or basic understanding of activities that the partner state chose itself independently.

EU – NATO cooperation

Cyber security cooperation between the European Union and NATO is mainly focused on issues related to cyber defence. To this end, the EU and NATO concluded a **Technical Arrangement on Cyber Defence** between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU), providing a framework for information and best practice exchange between emergency response teams, especially pertaining to cyber defence-related data. The

54 Participation of the Republic of Serbia in the Partnership for Peace Programme. Ministry of Foreign Affairs of the Republic of Serbia. http://www.mfa.gov.rs/en/foreign-policy/security-issues/partnership-for-peace-programme.

EU-NATO Joint Declaration[55] reaffirmed these efforts, stating the aim of expanding cooperation between the two bodies on cyber security and cyber defence including in the context of missions and operations, exercises and education and training. Enhanced EU-NATO cyber security cooperation is also promoted within the **EU's Global Strategy**[56].

Further stated priorities of cooperation between the two entities include fostering interoperability through coherent cyber defence requirements and standards, strengthening cooperation on training and exercises, and harmonising training requirements. To this end, further cooperation on countering hybrid threats is envisioned between the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch, as well as cyber defence exercises, with the involvement of the EEAS and other EU entities and relevant NATO counterparts, including the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.[57]

In terms of responding to crises, based on the Joint Framework on countering hybrid threats[58] and the Joint EU-NATO Declaration, a **European Centre of Excellence for Countering Hybrid Threats**[59] was inaugurated in 2017. Established as an intergovernmental think-tank under the auspices of EU and NATO, it is an instrument of its participating countries. Currently, Participants of the Memorandum of Understanding concerning Hybrid CoE[60] are Estonia, Finland, France, Germany, Latvia, Lithuania, Norway, Poland, Spain, Sweden, the UK and the USA. Participation in the Centre is open to EU Member States and NATO Allies. Hybrid CoE is to serve as a hub of expertise supporting the Participants' individual and collective efforts to enhance their civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security. It is intended that the Centre will offer this collective experience and expertise for the benefit of all Participants, as well as the EU and NATO. The Centre will follow a comprehensive, multinational, multidisciplinary and academic-based approach.

55 Joint Declaration by the resident of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation. 8.7.2016. European Council. http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

56 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. 2016. EEAS.

57 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. European Commission. JOIN(2017) 450 final.

58 Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. 6.4.2016. European Commission. JOIN(2016) 18 final.

59 The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/.

60 Memorandum of Understanding on the European Centre of Excellence for Countering Hybrid Threats. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2017/08/Hybrid-CoE-final-Mou-110417-1.pdf.

Organization for Security and Co-operation in Europe

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 Co-operation in Europe (OSCE) also deals with issues of cyber security, primarily in the form of fight against terrorism and cybercrime. In 2012, however, OSCE decided to step up individual and collective efforts to address security in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner.[61] To this end, an **informal working group on cyber security** has been established, tasked with drafting a set of confidence building measures to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs and to provide progress reports to the Chairperson of the Security Committee, who will report to the OSCE Permanent Council. The Republic of Serbia has a representative in the current composition of this informal working group.

In 2013, OSCE Member States adopted the first package of **Confidence Building Measures (CBMs)**[62] to reduce the risk of conflict caused by the use of information and communication technologies. The 11-measure package, among other things, includes exchange of information on cyber threats, national frameworks, strategies and terminology; providing security of and in the use of ICTs; holding consultations in order to reduce the risk of misperception and possible emergence of political or military tension or conflict that may stem from the use of ICTs and to protect critical national and international ICT infrastructure; 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.

A second set of measures[63], 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 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 protection of ICT-enabled critical infrastructure, providing several models of cooperation in this area.

Although adoption and implementation of 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.

---

61 Decision No.1039. Development of Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies. 26.4.2012. Organization for Security and Co-operation in Europe. PC.DEC/1039.

62 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 Co-operation in Europe. PC.DEC/1106.

63 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 Co-operation in Europe. PC.DEC/1202.

United Nations

The United Nations has been dealing with matters of information security through its **Office for Disarmament Affairs (UNODA)**[64] since 1998, when the Russian Federation introduced a draft resolution in the First Committee of the UN General Assembly. It was adopted without a vote and since then there have been annual reports by the Secretary General to the General Assembly with the views of Member States on the issue[65].

In addition, the **United Nations Institute for Disarmament Research (UNIDIR)** provides policy-focused capacity-building at the national, regional and multilateral level, as well as relevant research and analysis. UNIDIR also works to build awareness on how cyber-related initiatives interact with one another to ensure harmonious growth and development of a stable cyber environment. To this end, UNIDIR has thus far carried out an assessment of national capabilities, doctrine, organisation and transparency and confidence building for cyber security and provides workshops and conferences on international security and stability in terms of cyber. It also provides support to UN Groups of Governmental Experts working on matters of space and cyber.

Thus far, several iterations of the **Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security**, formed at the initiative of Member States, have examined the existing and potential threats from the cyber sphere and possible cooperative measures to address these. Main achievements of the GGE include outlining the global security agenda and introducing the principle that international law applies to the digital space. Thus far, through five GGEs progress has been made on reaching consensus and publishing three Reports on Developments in the Area of Information and Telecommunications in the Context of International Security. The work of the GGE from its first report in 2010 until today has positioned it as a key international mechanism for discussion – and, quite possibly, for reaching agreement - on standards and actions for confidence-building in cyberspace that states should seriously take into consideration. However, following failure to reach consensus within the fifth GGE, which discussed matters including existing and emerging threats; capacity-building; confidence-building; recommendations on the implementation of norms, rules and principles for responsible behaviour of States; application of international law to the use of information and communications technologies; and conclusions and recommendations for future work; the future of this framework is yet to be seen. The Republic of Serbia took part in the latest composition of the GGE, having one representative in the process.

In addition to the work conducted through the GGE, the United Nations International Telecommunications Union (ITU) publishes a **Global Cyber security Index (GCI)**[66], meas-

64 United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/.

65 Developments in the field of information and telecommunications in the context of international security. United Nations Office for Disarmament Affairs.

66 ITU drives global effort to strengthen cyber security: Global index measures national cyber security resilience. 2.4.2014. ITU. https://www.itu.int/net/pressoffice/press_releases/2014/16.aspx#.Uzxm-VyqxG4.

uring the status of cyber security worldwide. The GCI is a report compiled based on surveys that measure the commitment of Member States to cyber security, revolving around the five pillars of the ITU Global Cyber security Agenda – legal, technical, organisational, capacity building and cooperation. Based on research conducted during the course of 2016, the latest report covers all 193 ITU Member States[67]. According to this latest report, the Republic of Serbia is currently in a *maturing stage*, meaning complex commitments are already in place and the country engages in cyber security programmes and initiatives. With a GCI score of 0.311, the country is ranked 89th. To put in perspective, within the region, the Republic of Serbia is currently only ahead of Bosnia and Herzegovina (ranked 135th), preceded by Albania (ranked 88th), Montenegro (70st), Former Yugoslav Republic of Macedonia (54th), Hungary (51st), Bulgaria (44th), Romania (42nd) and Croatia (41st). All of these countries, however, are also defined as having *maturing* national cyber security frameworks.

67 Global Cyber security Index (GCI). 2017. ITU. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

Law on Information Security

The Law on Information Security[68] which the Republic of Serbia adopted on January 26, 2016, is the first umbrella law regulating measures for protection from security risks in information and communication systems, the responsibilities of legal entities in managing and operating information and communication systems, and determines competent authorities for implementation of protection measures.

Among the most important legal novelties is the establishment of the National Centre for Prevention of Security Risks, which is, according to international practice, a Computer Emergency Response Team (CERT), responsible for rapid reaction in case of incidents, as well as the collection and exchange of information on security risks to information and communication systems. The national CERT (nCERT) is under the jurisdiction of the Regulatory Agency for Electronic Communications and Postal Services (RATEL). Despite the lack of clear deadlines for its establishment within the Law, or mechanisms for securing necessary resources for efficient operation of the national CERT, the body has been established, although it is yet to achieve full operational capacity. One of the first steps towards this goal was the drafting of a comprehensive feasibility study for the establishment of a national CERT, in cooperation with the University of Belgrade Faculty of Electrical Engineering[69]. The study encompassed a normative and technical analysis of establishing and operating a CERT in terms of processes and procedures, a review of comparative practices in Europe and costs of implementation, an action plan as well as an overview of potential modalities of project funding from international funds that the Republic of Serbia has access to. Such a comprehensive approach can be considered as an example of application of the principles listed within the Law on Information Security referring to risk management and application of identified good practice. Establishing a national CERT is also one of the core obligations stemming from the EU NIS Directive, and an obligation of all Union Member States, posing thus also as a step that all candidate countries should have in mind.

68 Law on Information Security. *"Official Gazette of the Republic of Serbia"*, no. 6/2016.

69 Nešković, A. Krajnović, N. Nešković, N. 2016. Feasibility study for the establishment of a national CERT. Department of Telecommunications, Faculty of Electrical Engineering of the Belgrade University.

The Law also regulates issues such as the existence of ICT systems of special importance (essential services) and measures of their protection - which is an obligation in line with the NIS Directive - and provides the basis for regulating the field of cryptosecurity and compromised electromagnetic radiation protection, under the jurisdiction of the Ministry of Defence. Establishment of an information security inspectorate is also envisioned, tasked with overseeing the implementation of the Law and the work of ICT operators of essential services, under the jurisdiction of the competent ministry for matters related to information security, that is, the Ministry of Trade, Tourism and Telecommunications (MTT). However, even nearly two and a half years following the adoption of the Law on Information Security, the Inspectorate for Information Security, under the jurisdiction of the Department for Information Security and Electronic Commerce of the Ministry, is not fully established, which consequently means that no oversight of implementation of the Law is currently taking place.

Finally, the Law provides for the establishment of a Body for Coordination of Information Security Affairs (hereafter*: Body for Coordination*) - a body aimed at establishing cooperation and coordinated engagement in the national information security framework, as well as initiation and monitoring of preventive and other measures in the field. The Body for Coordination[70], although mainly an advisory actor as defined by the Law, provides an opportunity for a more comprehensive approach to information security, by recognising the possibility of setting up expert working groups in which representatives of other public institutions, the private sector, academic community and civil society can also take part. As such, the Body for Coordination presents the first official hint of political will to develop public-private partnerships for certain aspects of information security, which is not so common in the Republic of Serbia. It is particularly rare to have space for such a possibility within the law itself.

However, despite the unquestionable necessity of adopting a law that regulates the field of information security, certain areas are left insufficiently defined in the existing framework, which leaves space for individual interpretation, but may also present a potential security risk. Namely, although referring to the principle of risk management, the Law fails to explicitly prescribe risk analysis and assessment, or development of a methodology for conducting these, even though these should form the basis when deciding on adequate protection measures, designing and adopting an Act on Safety of ICT systems - which is an obligation of operators, or defining the role(s) of the national CERT and the CERT of public bodies, which provide early warning on risks and carry out tasks related to security risk prevention. Risk assessment is prescribed by Law only in the event of risk of compromising electromagnetic radiation, and only in the sense of assessing the risk of unauthorized access. When it comes to independent ICT operators, security analysis of ICT systems in terms of risk assessment, this action is only mentioned as a possibility, and not a clearly defined legal obligation.

70 Body for Coordination of Information Security Affairs was established by the Decision on the establishment of the Body for Coordination of Information Security Affairs, adopted on March 8, 2016. *"Official Gazette of the Republic of Serbia"* no.24/16 and 53/17.

When it comes to regulations that regulate the approach to information security in more detail, risk assessment is mentioned only by the Regulation on measures for protection of information and communication systems of special importance, analysed further below. However, this Regulation also fails to clearly define who is, and in what way, responsible for conducting risk assessment and how comprehensive this assessment should be. Without adequate risk assessment, it is unclear from the very outset what risks it is necessary to prevent, and which ones can be tolerated, which can in itself lead to inadequate distribution of resources for prevention and mitigation of incidents. Despite suggestions to have comprehensive risks assessment and analysis in the field of information security placed as one of the primary activities within the Strategy for the Development of Information Security, this deficiency has not been removed either by the bylaws adopted based on the Law, nor has any such objective been set out within the adopted Strategy, as is explained below.

In terms of incident response, the Law leaves information and coordination within the jurisdiction of the competent authority, that is, the Ministry of Trade, Tourism and Telecommunications, to a large extent, rather than the newly established national CERT, which unnecessarily bureaucratises operational mechanisms and additionally burdens an already overloaded ministry. The Protocol of Cooperation between the Ministry and RATEL envisions the establishment of communication channels for exchange of information on incidents that could have a significant impact on the violation of information security of ICT systems of essential services in the Republic of Serbia, as well as other incidents that are reported to the Ministry and RATEL.[71] According to the Protocol, both institutions are obliged to immediately forward and exchange notifications on incidents, consequences and activities undertaken in accordance with competencies determined by the Law on Information Security.

Although it is necessary to have a direct communication channel between the competent ministry and the national CERT, such a solution still fails to shorten the timespan needed to exchange information on an incident, nor does it essentially relieve the ministry itself. The same goes for the actors excluded from this Protocol, such as financial institutions, who submit notifications on incidents to the National Bank of Serbia. Having such solutions in place ignores the core essence of the existence of a national CERT as a sole, trusted operational and communication hub when it comes to incidents. The prescribed obligations therefore give primacy to respecting existing procedures and horizontal decision-making structures, instead of being based on principles of efficiency and rapid response, especially bearing in mind that critical infrastructures are at stake.

Overall, despite more than two and a half years since the adoption of the Law on Information Security, full implementation of the Law itself, and the adopted regulations, is still not established. There are several reasons for this state of affairs. Among them, the current ban on employment in the public sector makes it impossible to hire the necessary numbers of

71 Protocol on Cooperation between the Ministry of Trade, Tourism and Telecommunications and RATEL. 4.4.2018. Regulatory Agency for Electronic Communications and Postal Services. http://www.ratel.rs/information/news.134.html?article_id=2107.

professional staff to work in this field within state institutions. Additionally, the entire system within which the information security framework is set up, namely, the fact that it is under the jurisdiction of a multi-agency ministry (trade, tourism *and* telecommunications), narrows the space for adequately developing this field in the Republic of Serbia in a comprehensive and (primarily) time-efficient manner.

Adopted bylaws

With the adoption of bylaws, that is, regulations that determine provisions of the Law in a more detailed manner, in November 2016, the envisaged normative framework governing information security in the Republic of Serbia is officially completed. Adopting these bylaws, guided by the mentioned obligations as well as good practice examples, enabled certain shortcomings of the existing Law to be somewhat overcome. What is important now, however, is to have wider implementation of these regulations to commence as soon as possible, in order to test the prescribed solutions in practice and arrive at possible recommendations for specific amendments of the entire normative framework, in accordance with real needs and possibilities, at the same time bearing in mind international principles and obligations.

Regulation determining the list of activities in the fields in which activities of general interest are performed and in which information and communication systems of special importance are used. The Regulation determines which ICT systems fall into the category of systems of special importance, alongside the systems used in performing activities in public authorities, as well as systems for data processing that are considered particularly sensitive data in line with the law regulating personal data protection. Bearing in mind that the listed systems actually make up for critical information infrastructure - which is not defined as such due to the lack of a basic law regulating critical infrastructure - and the fact that the mentioned NIS Directive defines the types of operators (i.e. ICT systems) that are to be considered as systems of special importance (*operators of essential services*), the Regulation should be amended, or updated, in the medium term, to make it refer solely to systems that are truly of special importance. Namely, the NIS Directive prescribes that the criteria for identifying operators of essential services includes the following:

– the operator provides a service which is essential for the maintenance of critical societal and/or economic activities;

– the provision of that service depends on network and information systems; and

– an incident would have significant disruptive effects on the provision of that service.

The Directive also provides a more detailed list of possible operators that can be considered as of special importance within its Annex II. Here, systems used in the field of energy

(electricity, oil, gas), transport (air, rail, water and road), and banking are listed, alongside infrastructures of the financial market, health sector, supply and distribution of drinking water and digital infrastructures (such as internet exchange points - IXPs, internet providers - DNS hosting services, and internet domain name registries - TLD name registries).

In 2017, the European Commission proposed additional actors to be considered critical information infrastructure in order to further harmonise the process of identifying these at the EU level. To this end, the Commission also lists public administration, the postal sector, the food sector, chemical and nuclear industry, the environmental sector and civil protection[72].

Reviewing provisions of the Directive and its accompanying documents raises the question whether the list of activities defined within the Regulation in the fields in which activities of general interest are performed, and in which information and communication systems of special importance are used, is too extensive, that is, whether all the jobs it lists truly operate systems of special importance. Although the NIS Directive leaves states with space for determining wider lists, as well as adopting more stringent regulations for essential service operators, it is questionable whether it is expedient to engage all the actors listed in this Regulation, especially given the fact that systems of special importance at the same time also require special measures of security as well as special procedures. In this respect, and in order for clearer binding between individual laws and the overall normative framework, the given Regulations should be revised following the expected adoption of a Law on Critical Infrastructure, in order to determine a more precise list of critical information infrastructure, that is, ICT systems of special importance based upon which the (expected) identified national critical infrastructure depends. As a starting point, the Methodologies for the identification of Critical Information Infrastructure assets and services[73] developed by ENISA, can be used here for reference.

Regulation determining the measures for protection of information and communication systems of special importance. The Regulation closer determines the measures for protecting ICT systems, aimed at prevention and minimising damage from incidents that jeopardise the exercise of jurisdiction and performance, especially in terms of providing service to other entities, in accordance with the domains the protection measures refer to, as defined in Article 7 of the Law on Information Security. By defining each of the domains of protection in detail, the Regulation indicates the issues that operators of ICT systems of special importance are obliged to regulate.

However, despite the fact that the Regulation determined each protection measure individually, certain shortcoming still exist. Namely, in accordance with the mentioned principle of risk management, the Regulation prescribes, in Article 7, that the choice and level

72 Annex to the Communication from the Commission to the European Parliament and the Council. Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. COM(2017) 476 final/2 ANNEX 1.

73 Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks. 2014. ENISA.

of application of data protection measures is to be based on risk assessment, the need for risk prevention and the elimination of the consequences of the risk that has been materialised, including all types of extraordinary circumstances. Yet, as in the case of the Law itself, risk assessment is not at all regulated, that is, there is no definition of who, when and how carries it out when ICT systems of special importance are at stake, consequently making it unclear what the choice and level of application of security measures is based on.

Similarly, Article 12 of the Regulation determines that for the sake of secrecy, authenticity and integrity of data, an ICT system operator should consider employing adequate measures of crypto-protection. Once again, however, it is unclear based on what should the ICT operator base a decision if a comprehensive risk assessment has not been carried out previously, taking a baseline study on the vulnerability of the data, that is, the exposure of the data to risk as a starting point. In fact, the only risk analysis the Regulation determines is an analysis of ICT systems upon which an operator determined the level of exposure of ICT systems to potential weaknesses, defined within Article 20. This analysis is, however, first left undefined, and second, related only to an analysis of the systems in place, failing to officially prescribe any wider approach to analysis and assessment of the risks the operator is exposed to, even if this was potentially the intention of the legislator.

(Un)defined in this way, too much space is left to operators for individual interpretation, instead of clearly defining a legal obligation of conducting comprehensive and detailed analyses and assessments of risks, to also include elements such as data storage, data transfer, and even the levels of expertise and capacities of employees themselves. Based on the results of such an assessment, the length of time the personal data is stored for, and the protection of backup copies, the scope of these and the frequency of backup, as well as other measures for protection from data loss, determined by Article 17 of the Regulation, could all be defined. Within the current state of affairs, this is determined by the ICT system operator individually, and the Regulation fails to refer specifically to any concrete standard, practice or procedure based on which such a decision could be made, despite the fact that what is at stake are operators of ICT systems of special importance, that is, national critical information infrastructure.

Furthermore, the Regulation fails to determine the level of expertise of persons managing the ICT systems. Although these matters are most likely defined by internal acts, such as systematisations of positions within each operator individually, the formulation used within the Regulation in Article 4 is incomplete. Namely, the Regulation only defines that persons managing an ICT system, that is employees using the ICT system need to have an "adequate level of education and skills", without referring to internal acts or procedures in which the operator should clearly define what exactly an adequate level of education and skills implies.

Finally, Article 23 paragraph 3 of the Regulation determines that, in the event that data transfer takes place between an operator of an ICT system and an entity outside the operator, agreements on data transfer and confidentiality and non-disclosure agreements containing provisions on data security *can* be concluded. Once again, given that operators of ICT systems of special importance are at stake, it is of the utmost importance to cover all potential risks to the security of data, systems and the state, and in this light, a voluntary

obligation of concluding agreements with third entities outside the operators can potentially be considered a direct security risk. The Law on Information Security prescribes that an operator of ICT systems of special importance can entrust activities related to the ICT system to third persons, in which case the operator is *obliged* to regulate the relationship with those third persons in a such a way as to ensure implementation of measures for protection of that ICT system in accordance with the Law. Although in terms of this Regulation, entities outside the operator of ICT systems are not entrusted with any activities in terms of processing, storing and/or potential access to the data, only its transfer, it is unclear why the prescribed procedure differs, instead of recognising data transfer as an *activity* as defined by the Law. This would then, in accordance with the Law on Information Security, allow data transfers to take place only based on agreements adopted between the operator and the person this activity is entrusted to, or special regulations.

Regulation determining the content of the Security Act for information and communication systems of special importance, ways of verification and content of reports on security audits of information and communication systems of special importance. Despite previous suggestions and proposals[74], the Regulation determining the content of the Security Act is not based on the principle of risk management, and thus fails to define an obligation of primarily conducting a comprehensive risk analysis and assessment of ICT systems of special importance that the Act could be based upon. Still, the Regulation clearly refers to the content of the Security Act, determined by the list of protection measures defined within Article 7 paragraph 3 of the Law on Information Security. Furthermore, RATEL has in the meantime also developed a Model Security Act for ICT systems[75] which is publicly available and serves as a template for entering data on the specific operator.

However, the Regulation determines that the Act can also be a summarised document in case the measures it is to define are already contained in other acts of the operator of ICT systems. In this case, according to the Regulation, the Act is to contain provisions referring to these specific acts. Although the legislator's intention was clearly to avoid duplication and overlap of procedures, it is necessary to highlight that what is at stake here is a key document determining all measures of protection, principles, ways and procedures of achieving and maintaining an adequate level of security of critical information infrastructure systems, that is, ICT systems of special importance. In practice, this means that in the event of an incident, the Security Act should serve as an integral instruction on how to act at that given moment. If the Act contains only provisions that refer to further acts, as such, it fails to fulfil its basic purpose - to pose as a guide for crisis management in the case of an incident. Therefore, the recommendation would be to have absolutely all measures of protection, principles and procedures listed in this document in order to effectively manage crisis situations. This would at the same time ease the process of auditing and oversight of ICT systems, that is, reviewing the level of compliance of the Act itself with the Law and accompanying regulations, given that the inspector conducting the audit would only need to review one integral document instead of a number of related internal acts and procedures.

---

74 Rizmal, I. Radunović, V. Krivokapić, Đ. 2016. Guide through Information Security in the Republic of Serbia. OSCE Mission to Serbia. pp.35.

75 Model Security Act for ICT Systems. RATEL. http://ratel.rs/upload/documents/CERT/Model%20Akta%20o%20bezbednosti%20IKT%20sistema%20v.1.0.docx.

The Regulation also contains a provision determining an obligation to review the level of compliance of the Security Act and its application at least once a year. This is in line with recommendations and suggestions of the expert community presented during the public discussion on the normative framework of information security. It is determined that a review of ICT systems, that is, the review of compliance of applied security measures with the Security Act, the Law and the Regulation on the measures of protection, can be carried out by the ICT operators independently, or by engaging external experts. The level of expertise of the persons carrying out such reviews, however, is not defined, whether engaged internally or as an external expert. Consequently, the quality of the report on the measures of protection in place can be questioned, leaving at the same time space for potential security omissions and therefore risk.

Regulation on the procedure for submitting data, lists, types and significance of incidents and the procedure of notification on incidents in information and communication systems of special importance. The Regulation, in accordance with the Law, defines the incidents an operator is obliged to report, determining also a classification of incidents, which can be:

- Breaking into an ICT system;
- Data leakage;
- Unauthorised data modification;
- Data loss;
- Interruption in the functioning of the system of part of the system;
- Restricting accessibility of the service (DDoS attack);
- Installing malicious software within the ICT system;
- Unauthorised data collection through unauthorised supervision of communication or social engineering;
- Continuous attack on certain resources;
- Abuse of authority to access resources of the ICT systems; and
- Other incidents.

The Regulation is, however, unclear in certain parts, especially in terms of determining the types of incidents that are reported. Namely, it prescribes that incidents that, among other, "affect a large number of service users" are to be reported. What is considered as a large number of users is not defined. Bearing in mind that ICT systems of special importance are at stake, is, for example, limited availability of services of one sole user to be considered as a large enough number of users affected? The entire Ministry of Interior is, for example, considered as one user, while the unavailability of the Ministry's entire system indirectly affects all citizens within the country's borders, and even beyond.

Furthermore, Article 4 of the Regulation prescribes that an incident is reported in writing, without delay, and by the next working day at the latest[76]. Although this is in line with the NIS Directive, which leaves a maximum of 72 hours for reporting an incident, the question arises why this approach is not adopted in the Regulation itself, that is, why the deadline for reporting is not defined clearer.

This problem is also present in the decisions of the Law on Classified Information to which the Law on Information Security refers to, in case of incidents affecting classified data. Namely, the Law on Classified Data prescribes in Article 36 that the competent public authority is to be notified "without delay", who further notifies the Office of the National Security Council and Classified Information Protection on the measures taken to mitigate the damage and prevent recurrent incidents.[77] No clearer time period is defined within this law either.

Although normatively speaking, the adopted solutions do not constitute serious lapses in the normative framework overall, bearing in mind the importance of the field regulated by the laws and regulations adopted, one key recommendation for upcoming amendments of these documents is to determine cleared timeframes and deadlines for the fulfilment of legal obligations. Especially given the existence of clearly defined deadlines and criteria, in this case, in regulations adopted by the European Union, which the Republic of Serbia should bear in mind in the process of developing its national normative framework.

The determination of detailed conditions for checking compromising electromagnetic radiation and the ways of reviewing the risks of data leakage due to such radiation, as well as technical conditions for cryptographic algorithms, parameters, protocols and information assets in the field of cryptographic protection used in cryptographic products in the country to protect secrecy, integrity, authenticity and validity of data, is under the jurisdiction of the Ministry of Defence.

***

Although a certain degree of vagueness is necessary in regulations determining the rules for such a comprehensive field which, at the same time, encompasses large numbers of different entities (public bodies and institutions, telecommunications operators, the banking sector, etc.), the main challenge is the fact that vague provisions simultaneously create legal uncertainty and potential problems in practice. This is a consequence of the space left for arbitrary interpretation of certain provisions in the adopted normative documents. A possible transient solution could be to have a competent authority - the Ministry or the Body for Coordination - adopting opinions and recommendations related to closer regulating the given fields, which would act as guidelines for operators of ICT systems on how to interpret the currently vague normative provisions.

---

76 NB: In the event that an incident is detected, for example, on Friday, the question arising is whether in this case it can be reported as late as Monday?

77 Law on Classified Information. *"Official Gazette of the Republic of Serbia"* no.104/2009.

Strategy for the Development of Information Security

The Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020[78] (hereafter: *Strategy*), was adopted on May 29, 2017, envisioning the adoption of an accompanying Action Plan for its implementation within six months. The Strategy clearly defines the principles upon which the development of information security in the Republic of Serbia is based on, as well as priority areas that include the security of information and communication systems, security of citizens when using technology, fight against high-tech crime[79] and information security of the country.

As primary activities, the Strategy defines the development of a national CERT within RATEL, and a CERT of government authorities within the Government Administration for Joint Services of the Republic Bodies[80], the development of their capacities and the capacities of the Ministry of Trade, Tourism and Telecommunications as a whole, in this field.

Posing as a significant shift in the scope in which decision makers recognise the importance and need for basic knowledge of information and communication technologies by end-users (i.e. citizens), the Strategy calls for the need for developing *digital literacy* through the education system. Having in mind that in mid-2016, the National Education Council rejected proposals to introduce information security in the education system, the fact that following a decision of the same body, IT has been made a compulsory subject in elementary schools starting 2018, and that the Strategy defines that the education system should enable knowledge acquisition in the field of information security, is a significant step forward in efforts aimed at building capacities in information security of society as a whole - from elementary school to study programmes at universities.

The Strategy also recognises the need for extending national regulations on, and competencies of, the Office of the National Security Council and Classified Information Protection (hereafter: *NSA*) in terms of protection of classified information in ICT systems. Despite the fact the MTTT does not have the authority to regulate the functioning, competencies and capacities of other public bodies - in this case, the NSA - the fact that this issue was included in the Strategy indicates that the document applies a wider approach, taking into

78 Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020. *„Official Gazette of the Republic of Serbia"*, no.53/2017.

79 The Ministry of Interior is developing a separate strategy for the fight against high-tech crime (cybercrime). Matters related to high-tech crime are currently covered by the Strategy for the Development of Information Security, in accordance with requirements and obligations stemming from the process of accession negotiations with the European Union. Adopting a separate strategy to deal with high-tech crime will clearly separate the two fields, with crime-related matters expected to be generally removed from forthcoming updated of the strategy on information security. It is also one of the transitional measures of the accession process to the EU, agreed on within Chapter 24: Justice, freedom and security. For this reason, this publication does not go into analysing cybercrime-related matters in much detail.

80 With amendments to the Law on Information Security, this role has been acquired by another body - the Office for IT and e-Government, as explained further on.

account different areas that are related to the overall system of information security, highlighting the need for updating other normative frameworks in accordance with the adopted Law on Information Security.

Another positive development is having a clear definition of the need for adopting a national methodology for risk assessment, even though the Strategy envisions such an approach only in the case of ICT systems used for processing classified data. In accordance with the legally prescribed principle of risk management, as well as the selection and application of measures based on risk assessment, it is necessary to once more underline the need for adopting such an approach in all spheres of developing information security as defined by the Law, in order to ensure application of adequate, feasible and efficient security solutions.

It is of immense importance that the Strategy, within its baseline principles of developing information security, also recognises the need for establishing permanent cooperation between the public and private sectors, as a cornerstone for developing and building upon strategic priorities. In this sense, the Strategy recognises the need for the involvement of the private sector, citizens, the civil society and other relevant actors in the establishment of national information security system. The Strategy therefore adequately leaves the possibility of relative institutionalisation of this form of cooperation within the framework of special working groups of the Body for Coordination of Information Security Affairs provided for by the Law. The Strategy also emphasises that establishing public-private cooperation (PPP) within this framework enables efficient communication and optimisation of future activities, that is, timely exchange of information and resources sharing as another priority for developing information security in the Republic of Serbia. This is of special importance, especially having in mind existing capacities of the public sector. In this sense, the expert community has advocated for considering the possibility of establishing a *permanent expert working group* of the Body for Coordination within the process of developing a national action plan for the implementation of the Strategy. In this way, the envisioned public-private cooperation would be institutionalised, serving as a forum for exchange of knowledge, experience and information, that is, connecting all relevant actors from the public and private sector, as well as the academic community and civil society[81].

In addition to establishing a comprehensive framework of information security, such cross-sector cooperation is also recognised as an opportunity for undertaking certain activities aimed at development of products, processes and services for prevention and the provision of adequate levels of information security. To this end, the Strategy even indicates the need for institutionalising cooperation between the academic sector and competent authorities, with active participation of the private sector. Accordingly, the mentioned feasibility study for the establishment of a national CERT, developed in cooperation with the University of Belgrade Faculty of Electrical Engineering, can be understood as a step towards the application of the principles of cross-sector cooperation, in terms of recognising the capacities of the academic sector that can be utilised for the sake of developing the national framework of information security.

81 Rizmal, I. Radunović, V. Krivokapić, Đ. 2016. Guide through Information Security in the Republic of Serbia. OSCE Mission to Serbia. pp.60.

Office for IT and e-Government

In July 2017, the Government of the Republic of Serbia adopted a Regulation on the establishment of the Office for Information Technology and e-Government[82] which is the first time that an institution dealing with such matters is placed at this level of government. The Regulation stipulates that the Office carries out expert tasks related to: design, harmonisation, development and functioning of the system of electronic governance and information systems and infrastructure, development and application of standards in the introduction of information and communication technologies as well as support in the use of information and communication technologies in state administration bodies and government services; design, development, construction and maintenance of the computer network of public authorities; tasks for the needs of the Centre for the security of ICT systems in government authorities (CERT of government authorities, govCERT); providing services of designing, developing and operating internet access, internet services and other centralised electronic services; planning development and procurement of IT and communications equipment for the needs of state administration bodies and government services, as well as other tasks determined by special regulations.

The Office for IT and e-Government has therefore thus far focused mainly on the strategic objectives proclaimed by the Government, focused on developing e-Government services in the Republic of Serbia. To this end, projects that the Office focuses on include development of the e-Government portal, the infrastructure for issuing electronic time stamps (the RS-GOV TSA), and guidelines for developing websites and internet presentations of public institutions and bodies.

Law on the Amendments to the Law on Information Security

Latest amendments to the normative framework until the publication of this Guide refer to changes to the Law regulating the field. Namely, in October 2017, the Law on Amendments to the Law on Information Security was adopted, pertaining to Article 5 paragraph 1 of the Law. The amendments replace the reference to the Government Administration for Joint Services of the Republic Bodies with the term 'CERT of government authorities', whose tasks are carried out by the body in charge of 'design, development, construction and maintenance of the computer network of public authorities', in accordance with amendments of Article 2 paragraph 18. In practice, the CERT of government authorities (govCERT) is now placed within the jurisdiction of the mentioned Government Office for IT and e-Government of the Republic of Serbia.

82 Regulation on the Office for Information Technologies and Electronic Government. *„Official Gazette of the Republic of Serbia"*, no.73-2017.

Action Plan for the implementation of the Strategy for the Development of Information Security

The Action Plan for the implementation of the Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020 was adopted on August 28, 2018, with a timeframe covering the period 2018 to 2019[83]. Missing the primary deadline for adoption for almost a year, the adopted Action Plan introduces further inconsistencies within the strategic framework at the operational level, since its prescribed timeframe of two years has already lost eight months of its intended implementation.

Nevertheless, in line with the Strategy that it aims to operationalise, the Action Plan lists a number of positive and needed actions and developments.

Primarily, comprehensive capacity building efforts within the public sector are envisioned. These range from increased human resource capacity in terms of the number of staff directly engaged in the provisions and maintenance of security of national cyberspace and targeted training of staff at competent institutions, to raising general digital competences across the public sector. Development of specific guides and brochures on matters pertaining to data handling and safe use of ICT is also expected.

In terms of specific actions, the Action Plan envisions defining clear criteria for incident classification, mapping national critical information infrastructures, as well as development of applications for information exchange and cooperation among all registered CERTs in case of an incident. Establishment of a special CERT of the Ministry of Foreign Affairs is also listed, as well as setting up of the Inspectorate for Information Security, as envisioned by the previously adopted Strategy. Finally, the Action Plan prescribes carrying out annual analyses of cyberspace threats and provisions of recommendations for risk mitigation. Following the previously mentioned principles of risk analysis and assessment, such analyses will hopefully also contain analyses of risks, including existing capacities and capabilities, and not just external threats.

As for early national capacity development, introducing programmes at primary and secondary school levels of education is envisioned, analysing, in parallel, the possibilities of establishing specialised cyber security curricula at university level. Although the Action Plan does not further elaborate on what such programmes would entail, specifically in the case of university programmes, attention should be paid to exploring the potential of having multidisciplinary study programmes on cyber security, combining both policy and technical aspects of the field. The potential of the academic sector to contribute to national research and development efforts is also recognised, and is something that, according to the Action Plan, will be further explored.

---

83 Government Conclusion no. 345-7654/2018-1. 28.8.2018. Government of the Republic of Serbia.

The Action Plan also envisions amendments to the normative framework. First of all, amendments of the Law on Information Security are to take place, in order to make it fully aligned with EU directives and regulations. This is to be complemented by amendments to other laws that are also influenced by cyber security considerations, namely, the Law on Classified Information Protection and the Law on Personal Data Protection.

Broader efforts prescribed by the Action Plan refer to carrying out both general, comprehensive as well as targeted awareness raising campaigns. These refer to informing the general public on the potentials, risks as well as responsibilities related to the use of ICT, but also more specific awareness raising programmes targeting the public sector, the private sector, and children, parents and teachers as three different groups of stakeholders needed different scope, type and level of information.

Foreign policy matters are also covered by the Action Plan. International cooperation is envisioned, through cooperation of state CERTs with their foreign counterparts and their engagement in international CERT organisations, as well as through participation in civilian and military cyber drills and exercises. Participation in international cyber exercises however, both civilian and military, is to be coordinated by the Ministry of Defence solely, with other ministries and security agencies listed only as partners, including the Ministry of Foreign Affairs. This is a potentially ineffective solution in the longer run as the Ministry of Defence is, in accordance with the Action Plan, tasked to coordinate participation of civilian representative of the country, such as representatives of the Cybercrime Unit of the Ministry of Interior, or the nCERT to that matter.

Although most of the activities listed in the Action Plan seem realistic and in line with existing capacities and capabilities, the document's greatest flaw stems from the prescribed deadlines for implementation. Alongside the fact that the Action Plan covers the period from 2018 to 2019, meaning eight months of its implementation period have already been lost waiting for its adoption, some of the deadlines set for specific activities are set retroactively. This is the case, for example, with the task of defining criteria for incident classification, or developing the Inspectorate for Information Security at the MTTT, where the deadlines are set for the second quartile of 2018 – two months before the Action Plan was adopted. Additionally, it is indicative that all listed deadlines are solely for the year 2018, with the exception of activities that are to take place on a continuous basis and some budget allocations for both years. Given that the implementation period also encompasses the year 2019, it is unclear what specific activities are to take place during this year.

***

A significant step forward, deserving special mention, refers to public-private partnership. Despite the fact that in terms of concrete activities, the document recognises the private sector mainly as contributing only to research and development and capacity building through joint efforts, at the same time, space is left for building stronger public-private cooperation within the framework provided by the Body for Coordination. Namely, the Action Plan clearly states the intention to make use of envisioned expert working groups that can be established within the Body for Coordination, to be composed of representatives of the public and private sector, the academic community and civil society. This is an operative

solution that the expert public composed of representatives of all of these stakeholders has been calling for ever since the adoption of the Law on Information Security[84]. Although establishing such groups on a *permanent* basis has been advocated for, and the Action Plan does not prescribe a concrete timeframe[85], having such a formulation built into the document is in itself a success. It demonstrates continuation of political will to cooperate and work with various relevant stakeholders in efforts to further develop cyber security in Serbia, but also poses as a modest success of the existing, informal, public-private partnership endeavour in the country.

A public-private partnership for cyber security in Serbia: The Petnica Group

Parallel to the establishment of a normative framework, an informal, operational framework has been developing. Namely, following several smaller activities held over the course of 2014, three international organisations commenced a series of joint activities aimed at encouraging development of a comprehensive framework of cyber security in the Republic of Serbia. To this end, in mid-2015, the OSCE Mission to Serbia, DiploFoundation and the Geneva Centre for the Democratic Control of Armed Forces (DCAF) set up a strategic partnership with the Petnica Science Centre and organised a coordination meeting of key public and private stakeholders in the field of cyber security. The meeting marked the formation of the so-called "Petnica Group", which, through several phases, developed into an informal, multi-actor, public-private cooperation group composed of representatives of key national cyber security stakeholders from the public and private sector, academia and civil society[86]. Since its inception, the Group has focused on strengthening public-private cooperation and developing adequate policies and strategic frameworks in the field of cyber security in the Republic of Serbia.

Over the years, the Petnica Group met regularly at the Petnica Science Centre, discussing ongoing policy developments, issues and challenges ranging from the normative framework developed during the course of 2015-2016, national strategic priorities related to the preparation and adoption of the national Strategy for the Development of Information Security, as well as needed and possible modalities of cooperation in the field of cyber security. The Group also conducted the first national policy-focused cyber drill. Additionally, activities within this public-private framework saw over a dozen different national and regional events related to cyber security, gathering over one hundred and fifty participants from key ministries and agencies, members of parliament, representatives

84 Rizmal, I. Radunović, V. Krivokapić, Đ. 2016. Guide through Information Security in the Republic of Serbia. OSCE Mission to Serbia. pp.60.

85 According to the Law on Information Security, expert working groups are to be issue-based and established in an ad-hoc manner.

86 Members of the Petnica Group are listed in Annex I.

of the private sector, academia, civil society organisations and the media. In addition, international best practice exchange was made possible with partners from Finland, Israel, Montenegro, Poland, Slovenia, Switzerland and the United States, as well as institutions such as the Belfer Centre for Science and International Relations of the Harvard Kennedy School, Geneva Centre for Security Policy, George C. Marshall Centre's European Centre for Security Studies, European Union Network and Information Security Agency (ENISA) and the International Telecommunications Union.

Petnica Group's focus on policymaking provides a missing channel for the technical community and operational level staff to highlight existing normative regulations potentially posing as obstacles in practice. It acts as a bridge between the technical community and policy decision makers, fostering a platform for reaching proposals for joint solutions. Some of these solutions already managed to find their way into final versions of adopted normative and strategic frameworks and succeeding policy deliberations. What this framework also provides is development of a comprehensive mutual understanding of other actors' jurisdictions and competencies in the national cyber security framework. As a result, the Petnica Group acts as a genuine hub for information, knowledge and practice exchange; a support group in case of an incident, due to the personal contacts established between its members; as well as a pool of potential partners on future projects and programmes in cyber security.

Practice makes perfect: First national policy-focused cyber drill

Continuing efforts aimed at developing efficient communication and cooperation between the public and private sector(s) in cyber security in the Republic of Serbia, the OSCE Mission to Serbia supported the organisation of the first ever national policy-focused cyber drill. The drill focused on testing existing communication procedures as well as those under development, in case of a national cyber incident. Focus was placed on whether these procedures are realistic, whether existing capacities enable their implementation, and the timeframe needed for isolating or resolving a given incident if these are applied.

The drill was therefore tailor-made to existing circumstances, based on obligations stipulated by the Law on Information Security in force, complementary bylaws and amendments, as well as principles prescribed by the Strategy for the Development of Information Security. All of these documents determine the obligation of establishing communication procedures in case of a cyber incident or threats to national cyberspace. Through simulating practical application of this framework, the drill analysed the efficiency of existing procedures for crisis management, as well as the readiness of key public and private actors to apply these, highlighting good practice but also existing and potential challenges and obstacles in crisis communication.

The end result of the drill was three-fold. First, participants of the drill had the opportunity to exchange knowledge and experience on mutual procedures and capacities in order to establish more efficient communication in the future. Second, the drill enabled a review of the sustainability and efficiency of the existing normative framework, procedures and practice in a situation simulating a possible real-life incident. Finally, with the conclusions and recommendations from the drill presented to key decision makers within a detailed report, the drill enabled fulfilment of its third aim, that is, raising awareness and providing information upon which representatives of public institutions will be able to base their decisions and focus their efforts in the future.

Some of the key conclusions and recommendations resulting from the drill include the need for:

– Codifying communication channels and responsible persons;

– Establishing intensive public-private cooperation in terms of shared capacities and resources;

– Determining clear criteria for classification of incidents;

– Inspecting the opportunity for establishing a central, operational crisis centre in case of a national cyber incident through standard operating procedures;

– Determining clear procedures for communication with the public depending on the type of incident; and

– Defining the jurisdiction of national contact points/persons for cooperation in international organisations and the scope of their operations.

An integral version of the drill report was presented to key national decision makers, representatives of key institutions in charge of matters pertaining to the national cyber security framework. The report, in addition to an explanation of the drill itself and detailed conclusions and recommendations, also contained an overview of key challenges and obstacles arising from the existing normative framework and realistic capacities of the actors involved. This presentation took place at a closed meeting and the integral version of the report has not been made public, as it includes sensitive information on potential vulnerabilities. Publicly available information on how the drill was contemplated, as well as the key conclusions and recommendations resulting from it, is available in Annex II.

OPPORTUNITIES

European Union

Covering the period between 2014 and 2020, **Horizon 2020**[87] is the largest EU research and innovation funding programme adopted thus far, with a budget totalling 77 billion Euros. The current Work Programme[88] covers the period between 2018 and 2020, with an investment budget of around 30 billion Euros, listing five major priorities.

Under the *Integrating digitization in all industrial technologies and societal challenges* priority, focus is placed on "Digitising and transforming European industry and services". Here, the Programme aims to support the Digital Single Market Strategy by focusing on combining digital technologies (big data, internet of things, 5G, high performance computing etc.) with other advanced technologies and service innovation. "Open Science" is also to be promoted, focusing on an 'Open Research Data' approach and the creation of a European Open Science Cloud, fostering the stewardship and re-use of research data and tools across disciplinary and geographical borders.

Efforts aimed at fostering *Societal Resilience*, underline that ensuring cyber security requires looking at vulnerabilities of critical infrastructures and digital services and calls for new technological as well as non-technological solutions, so that the full economic and social potential of digital technologies can be safely exploited. A dedicated focus area "Boosting the effectiveness of the Security Union", aims to directly respond to identified security challenges, most notably, reinforcing European cyber security technology and industrial capacity. This activity is in line with challenges previously identified by the Commission[89]. Certain Horizon 2020 resources will thus be directed towards developing the envisioned European network of cyber security Competence Centres. Activities within this initiative already commenced, with a survey indexing European cyber security centres of expertise (including universities, research centres, and the like). The results of this mapping will be translated into a "Cyber security Atlas" (an index of existing EU cyber security

87 Horizon 2020. European Commission. https://ec.europa.eu/programmes/horizon2020/en.

88 Horizon 2020 Work Programme 2018-2020. European Commission Decision C(2017) 7124 of 27 October 2017.

89 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

Centres), forming a tool for identifying potential partners and pooling resources among the cyber security community.[90]

The Republic of 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 programmatic blocks and topics of Horizon 2020. This is done through an established network of National Contact Persons[91], allocated with specific Horizon focus areas.

One of the key preconditions for taking part in Horizon 2020 projects is having a consortium of institutions across eligible countries, most often comprising of different types of actors - from the government, to the private, civil and academic sectors. While this brings a certain complexity in terms of preparation and implementation of a project, it also brings direct benefits in the form of exchange of experiences among countries and actors and strengthens cooperation between them.

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)[92], which annually allocates around 200 million Euros for Serbia. IPA II takes up a sectoral approach in planning activities during the implementation period. It is directed at a smaller number of strategic sectors identified by IPA II beneficiary countries together with EU institutions and defined by the Sector Planning Document (SPD) for the respective country. These sectors, among other, include the issue of internal affairs, within which – in Serbia's case – the need for supporting the fight against cybercrime has been recognized.[93]

As part of this instrument, there is an additional EU fund, the so-called **Multi-Country IPA**[94]. It looks towards strengthening regional cooperation in certain sectors, enabling participation of each country in the region, and reducing costs. One of the programme's priorities is the fight against organized crime including also the fight against cybercrime. Here, the EU relies on Council of Europe capacities, and is currently implementing the iPROCEEDS project (2016-2019)[95]. iPROCEEDS 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 via the internet. Participating countries include Albania, Bosnia and Herzegovina, Montenegro, Serbia, the Former Yugoslav Republic of Macedonia, Turkey and Kosovo*.

---

90 Survey indexing the European cyber security centres of expertise. EUSurvey. https://ec.europa.eu/eusurvey/runner/cyber security-survey.

91 National Contact Persons. Horizon 2020. Ministry of Education, Science and Technological Development. http://horizon2020.mpn.gov.rs/pocetna/nacionalne-kontakt-osobe/.

92 Instrument for Pre-Accession Assistance. European Neighbourhood Policy and Enlargement Negotiations. European Commission. https://ec.europa.eu/neighbourhood-enlargement/instruments/overview_en.

93 Instrument for Pre-Accession Assistance (IPA II). Indicative Strategy Paper for Serbia (2014-2020). Adopted on 19.8.2014. https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2014/20140919-csp-serbia.pdf.

94 Multi-country – financial assistance under IPA II. European Neighbourhood Policy and Enlargement Negotiations. European Commission. https://ec.europa.eu/neighbourhood-enlargement/instruments/multi-beneficiary-programme_en.

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

Within the framework of its **Instrument contributing to Stability and Peace (IcSP)**[96], the European Commission funds EU actions in the field 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. Strategically, the Instrument aligns itself with priority areas indicated by the European Strategy for Cyber Security, especially in aspects related to the fight against cybercrime.[97] In terms of matters directly pertaining to cyber security, activities including raising awareness on cyber threats; developing national cyber security strategies; providing for information assurance and resilience; setting up, training and equipping Computer Emergency Response Teams (CERTs), building early warning, information sharing and analysis capabilities in priority regions, are all listed as potentially to be funded through the Instrument. From 2014-2016, a pilot project related to cyber security was implemented with the support of IcSP, covering the Former Yugoslav Republic of Macedonia, Kosovo* and Moldova[98], albeit with mixed results.

In 2016 the Commission adopted an Annual Work Programme[99] for this Instrument, setting out activities related to cyber security to be rolled out over a period of 72 months (six years). The document envisions the following results:

– Increased awareness of decision-makers on cyber security issues and adoption of consistent, actionable national cyber strategies in priority countries by fostering a multistakeholder approach and promoting the establishment of appropriate coordination frameworks and structures amongst public sector entities themselves and also with the private sector, both at policy and operational levels;

– Increased local operational capacities to adequately prevent, respond to and address cyber-attacks and/or accidental failures through strengthened Computer Emergency Response Teams and improved formal and informal cooperation in the national cyber ecosystem of third countries; and

– Increased trust and enhanced regional, trans-regional and international cooperation on cyber security issues through the promotion of formal and informal networks for sharing of best practices and incident information.

The Fund requires participation of actors from different regions. The Republic of 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. Despite the fact that the Annual Work

96 Instrument contributing to Stability and Peace*, preventing conflict around the world. Service for Foreign Policy Instruments (FPI). European Commission. http://ec.europa.eu/dgs/fpi/what-we-do/instrument_contributing_to_stability_and_peace_en.htm.

97 Instrument contributing to Stability and Peace (IcSP). Thematic Strategy Paper (2014-2020). Multi-annual Indicative Programme 2014-2020 (Annex).

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

99 Annex III of the Commission Implementing Decision on the Annual Action Programme 2016 for Article 5 of the Instrument contributing to Stability and Peace to be financed from the general budget of the Union. Action Document for Protecting Critical Infrastructure.

Programme for 2017[100] failed to include activities directly related to cyber security, given the strategic framework and results of the mentioned pilot scheme run in the preceding period, this programme should be monitored for potential opportunities in this field in the years to come.

The Republic of Serbia also has access to the EU **Erasmus+ programme**[101] which includes financing activities aimed at creating knowledge alliances among institutions of higher education and the development of their capacities. As a general rule, the Programme operates by supporting strategic partnerships, targeting cooperation between organisations established in Programme and Partner Countries. The Republic of Serbia falls within the latter category, within Region 1 (Western Balkans). The country can engage in projects through several modalities, depending on the specific action - as coordinator, partner, and/or partner that brings added value.[102]. Strategic partnerships may also involve associated partners from the public and private sector. The 2018 Erasmus+ Programme Guide[103] lists, among other, activities to increase the uptake of subjects where skills shortages exist and improve career guidance; designing and developing curricula that meet the learning needs of students that are relevant to the labour market and societal needs, including through better use of open and online, blended, work-based, multi-disciplinary learning and new assessment models; developing, implementing and testing the effectiveness of approaches to promote creativity, entrepreneurial thinking and skills for applying innovative ideas in practice; and supporting the transfer of latest research outputs back into education as input for teaching; as activities to be given priority.

One of the national Erasmus+ priorities in the 2017 call for Capacity Building in the field of Higher Education (CHBE) was *information security services*. To this end, two Erasmus+ CBHE project grants were awarded in the field of information security, one to the University of Novi Sad (UNS) and another to the Academy of Criminalistics and Police Studies, in August 2017. In December 2017 the UNS organized a kick-off meeting of the "Information Security Services Education in Serbia (ISSES)" project. The project consortium consists of four Serbian higher education institutions: the University of Novi Sad, University of Belgrade, University of Niš and Subotica Tech. Foreign partners include some of the most prestigious technical universities in nearby EU countries, namely the CrySys Lab of the Budapest University of Technology and Economics (Hungary), Politecnico di Milano (Italy) and the University of Zagreb (Croatia). The consortium also takes inputs from relevant industrial partners in Serbia and Hungary, including Unicom-Telecom, Eccentrix, Cisco, Execom. The project's primary goal is to improve educational capacities of Serbian Higher Education Institutions (HEIs) in the field of Information Security Services. The project partners will collaborate to develop 13 new information security courses, and design 4 types of information security laboratories, based on which the four Serbian HEI partners will build 7 state-of-the-art information security laboratories. Additionally, the Serbian HEIs

100 Commission implementing decision of 26.6.2017. on the annual action programme 2017 for the Instrument contributing to Stability and Peace – Conflict prevention, peace-building and crisis preparedness component to be financed from the general budget of the European Union. European Commission. C(2017) 4278 final.

101 Erasmus+. European Commission. https://ec.europa.eu/programmes/erasmus-plus/node_en.

102 Position of Serbia. Tempus Foundation. Erasmus+. http://erasmusplus.rs/erasmusplus/position-of-serbia/.

103 Erasmus+ Programme Guide 2018. 25.10.2017. European Commission.

will introduce new MSc study programmes in critical infrastructure security, digital forensics, as well as cloud and internet of things (IoT) security. The second Erasmus+ awarded project, "Improving Academic and Professional Education Capacity in Serbia in the Area of Safety & Security (by Means of Strategic Partnership with the EU) (ImprESS)", is coordinated by the Academy of Criminalistics and Police Studies in Belgrade. The project's main objective is to improve Serbian and regional capacity in terms of infrastructure, human potential as well as cooperation in the area of safety and security in order to prevent and efficiently manage crises and hazards and to develop a dedicated European Ecosystem for training of highly qualified experts who will ensure implementation of adequate procedures in line with EU regulation.

In addition, the Erasmus+ Programme also states that in order to better support students to acquire the skills necessary for their future, a partnership between the Erasmus+ and Horizon 2020 programmes has been established. This partnership will provide traineeship opportunities for students and recent graduates who wish to acquire digital skills in subjects including digital marketing (e.g. social media management, web analytics); digital graphical, mechanical or architectural design; development of apps, software, scripts, or websites; installation, maintenance and management of IT systems and networks; cyber security; data analytics, mining and visualisation; programming and training of robots and artificial intelligence applications. The traineeships are expected to take place in the EU Member States as well as in Horizon 2020 associated countries, of which the Republic of Serbia is one.

The **European Defence Agency (EDA)**[104], supports EU Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future. Within its key capability programmes, EDA lists four priority areas of which cyber defence is one. The Agency's Capability Development Plan also lists cyber security as one of its priority actions. Cyber matters are approached through focus on training and exercises, cyber situation awareness, advanced persistent threat (APT) detection, digital forensics for military use and the development of a Cyber Defence Strategic Research Agenda (CSRA).[105] Based on an Administrative Agreement the Republic of Serbia concluded with the Agency, as of 2013 the country is able to participate in EDA's projects and programmes. Thus far, however, the country has used this opportunity only once, in 2016, joining the project *EU Satcom Market*[106].

Additionally, the Cyber security Digital Service Infrastructures (DSI) programme of the **Connecting Europe Facility (CEF)**[107] can provide for significant EU funding in assisting Member State CSIRTs to improve their capabilities and cooperate with each other

104 European Defence Agency. https://www.eda.europa.eu/home.

105 Cyber Defence. 5.9.2017. European Defence Agency. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence.

106 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.

107 Connecting Europe Facility (CEF). Innovation and Networks Executive Agency (INEA). European Commission. https://ec.europa.eu/inea/en/connecting-europe-facility.

through an information exchange cooperation mechanism.[108] Managed by the Innovation and Networks Executive Agency (INEA) of the European Commission, the CEF Telecom strand provides for 1.04 billion Euros for the telecommunications sector for the period 2014-2020.[109] The DSIs from which funding is foreseen in 2018 include Europeana and Safer Internet, as well as eIdentification and eSignature, eDelivery, eInvoicing, Public Open Data, Automated Translation, Cyber security, eProcurement, On-line Dispute Resolution (ODR), Business Registers Interconnection System (BRIS), eHealth, Electronic Exchange of Social Security Information (EESSI) and the European eJustice portal.[110] Among these, the Safer Internet service infrastructure focuses on deployment of services that help make the Internet a trusted environment for children by providing an infrastructure to share resources, services and practices between national Safer Internet Centres (SICs) and to provide services to their users, including industry. Likewise, activities pertaining directly to cyber security are focused on support to critical digital infrastructures. Here, focus is placed on the establishment and deployment of a core cooperation platform of cooperation mechanisms initially focused on Computer Security Incident Response Teams (CSIRTs) in accordance with the NIS Directive.[111]

Recently, the European Commission published that CEF's objective is to establish an enabling facility for a series of European level sectoral ISACs (Information Sharing and Analysis Centres) with industry and NIS Directive stakeholders for improved awareness and preparedness of cyber security risks and threats. Support under CEF's Generic Services is being broadened out to encompass not only CSIRTs but also operators of essential services, digital service providers and national competent authorities under the NIS Directive.[112]

For the time being, participation of candidate countries like the Republic of Serbia is under the same conditions as third and acceding countries – they are eligible for participation as part of a consortium with applicants from EU Member States/EEA countries, where their participation is deemed indispensable to achieve the objectives of a given project of common interest.

***

108 Annex to the Communication from the Commission to the European Parliament and the Council. Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of network and information systems across the Union. 13.9.2017. COM(2017) 476 final. ANNEX 1.

109 Calls. Innovation and Networks Executive Agency (INEA). European Commission. https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding.

110 Annex to the Commission Implementing Decision on the adoption of the work programme for 2018 and on the financing of Connecting Europe Facility (CEF) – Telecommunications Sector. 5.2.2018. European Commission. C(2018) 568 final.

111 Section 3.2 and Section 3.8. Annex to the Commission Implementing Decision on the adoption of the work programme for 2018 and on the financing of Connecting Europe Facility (CEF) – Telecommunications Sector. 5.2.2018. European Commission. C(2018) 568 final.

112 Connecting Europe Facility supports expansion of cyber security capabilities. 27.3.2018. European Commission. https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facility-supports-expansion-cyber security-capabilities.

Apart from opportunities for obtaining resources for, and/or engaging in, development and capacity building, the Republic of Serbia also has access to mechanisms for engaging in partnership development, further cooperation and standardization.

First of all, the Republic of Serbia, that is, companies, enterprises, organisations, and other stakeholders from the country, are eligible for membership in the **European Cyber Security Organisation (ECSO)**[113]. As mentioned, ECSO is the contractual counterpart to the European Commission for implementation of the contractual Public-Private Partnership (cPPP). Its membership ranges from large companies, small and medium-size enterprises and start-ups, to research centres, universities, end-users, operators, clusters and associations, as well as local, regional and national administrations. Membership in ECSO is open to legal entities established in an ECSO country, that is, countries that are EU Member States, EEA/EFTA countries, as well as Horizon 2020 associated countries, of which the Republic of Serbia is one.

Further engagement in processes pertaining to policy development and input is provided in matters related to standardization. Serbia's Institute for Standardisation[114] is a member of the **European Committee for Standardisation (CEN)**[115], which brings together national bodies for standardization from 34 European countries. CEN has already been recognized as an important transnational European Standardisation Organisation (ESO) fostering continuous exchange of information and good practices in order to harmonize regional (European) and international (ISO) standards. Standardization has, in general, featured prominently in recent strategic documents of the Union, namely the Regulation proposal on Information and Communication Technology cyber security certification[116]. To this end, an envisioned reformed and strengthened ENISA is expected to regularly contribute to the work of cyber security working groups of ESOs.

CEN membership also enables participation in the CEN/CENELEC Focus Groups on Cyber security established in 2016, which will support both CEN and CENELEC to explore ways and means for supporting the growth of the Digital Single market. It will analyse technology developments and develop a set of recommendations to its parent bodies for international standards setting.[117] To this end, the Focus Group, for example, looked into the different usages/meanings of the term 'cyber security' by various stakeholders in different standards and finalized a document 'Definition of Cyber security'[118] consisting of an overview of overlaps and gaps of those definitions, with a view of moving towards a

113 European Cyber Security Organisation. https://www.ecs-org.eu/.

114 Institute for Standardisation of Serbia. http://www.iss.rs/en.

115 European Committee for Standardisation. https://standards.cen.eu/index.html.

116 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cyber security certification ("Cyber security Act"). European Commission. COM(2017) 477 final. 2017/0225 (COD).

117 Cyber security. CEN/CENELEC. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cyber security.aspx.

118 CSCG Recommendation #2 – Definition of Cyber security. Cyber Security Focus Group. CEN/CENELEC. V1.8.

common understanding of the cyber security domain. The Group also liaises with ENISA and the Multi-Stakeholder Platform on ICT standardisation[119].

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.[120] 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)[121]. EFSI is not an independent body. It is an initiative jointly launched by the European Investment Bank Group and the European Commission, aimed at mobilising private investment in projects that are strategically important for the EU. The first cyber security finance contract, worth 20 million Euros, was signed in 2017 with France's CS Communication & Systèmes (CS) Group to support the implementation of its 2017-2021 research and development programme.[122] When it comes to the Republic of Serbia, EIB has thus far financed mainly the transport sector, but recently shifted its focus towards small and medium-size enterprises to help boost growth and job creation.[123] The Republic of Serbia is eligible for EFSI programme resources as part of the EU's "enlargement region"[124]. Taking this into account, following the expected establishment of the Cyber Security Investment Platform within the European Fund for Strategic Investments, possibilities for cooperation within this framework should be sought.

Additionally, the Commission intends to 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.[125]

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. Its existing mechanism of Smart Specialisation Platforms[126] has thus far dealt with the notion of EU investment in ICT, but this is a field yet to be monitored in terms of cooperation and engagement opportunities.

---

119 An advisory expert group on all matters related to European ICT standardisation. European Multi Stakeholder Platform on ICT Standardisation. https://ec.europa.eu/digital-single-market/european-multi-stakeholder-platform-ict-standardisation.

120 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 Competitive and Innovative Cyber security Industry. 5.7.2016. European Commission. COM(2016) 410 final.

121 European Fund for Strategic Investment (EFSI). European Investment Bank. http://www.eib.org/efsi/.

122 Juncker Plan - First EIB financing for cyber security in France. 2.10.2017. European Investment Bank. http://www.eib.org/infocentre/press/releases/all/2017/2017-261-plan-juncker-1er-financement-de-la-bei-dans-le-domaine-de-la-cybersecurite-en-france.htm?f=search&media=search.

123 Serbia. European Investment Bank. http://www.eib.org/projects/regions/enlargement/the-western-balkans/serbia/index.htm.

124 Enlargement countries. European Investment Bank. http://www.eib.org/projects/regions/enlargement/index.htm.

125 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 Competitive and Innovative Cyber security Industry. 5.7.2016. European Commission. COM(2016) 410 final.

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

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, among other, needs highlighted within the Alliance's Strategic Concept. Accordingly, SPS priorities in this field focus on protection of critical infrastructure, in terms of developing cyber defence capacity and policies; support in developing cyber defence capabilities, including new technologies and support for construction of information infrastructure; and raising awareness about the situation in this field.[127] Participation in the SPS program is open to both NATO member states and partner countries. Projects funded under this program are led by a NATO member state, with at least one more partner country. The Republic of Serbia obtained partner status in 2006.

Additionally, within the country's Individual Partnership Action Plan for 2015-2016, the Ministry of Foreign Affairs of the Republic of Serbia 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.[128] In late 2017, civil servants from the Office of the National Security Council and Classified Information Protection of the Serbian Government were trained to deal with information systems security (INFOSEC) in real life situations, within the Science for Peace and Security (SPS) Programme. The course addressed specific cyber security concerns, such as crisis management and protection of classified information that the participants have encountered or are currently dealing with. They learned how to develop and implement specific toolkits and roadmaps to address INFOSEC policies within an institutional framework. The participants also learned best practice approaches that help managers to track, plan and monitor activities in implementing INFOSEC within their organisations.[129]

The SPS Programmes enable partner country scientists to increase contacts in the NATO science community, while building a stronger science infrastructure in their home countries through multi-year research and development programmes and provides advanced level training courses and research workshops.[130] Currently, the Republic of Serbia is engaged in SPS programs related to cyber defence, defence against chemical, biological, radiological and nuclear (CBRN) agents, counter-terrorism, the Women, Peace and Security agenda, energy, and environmental security.

***

127 SPS key priorities. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/85291.htm.

128 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.

129 NATO trains Serbian civil servants in cyber defence. 23.11.2017. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/news_149194.htm?selectedLocale=en.

130 What we fund: SPS Grant Mechanisms. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natolive/87260.htm.

In addition, there is the **NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE)**[131]. NATO CCDCoE is a NATO accredited centre of knowledge, *think-tank* and centre for training focused on interdisciplinary applied research and development, as well as on consulting services, training and courses in the field of cyber security. The Centre's mission is to enhance capability, cooperation and information-sharing between NATO, Allies and partners in cyber defence. It 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.

The Centre is neither a part of the NATO command structure nor financed from the NATO budget. Instead, it is staffed and financed by its (currently twenty-one) member nations. Membership of the Centre is open to all Allies. Currently, Austria, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States have signed on as Sponsoring Nations of the Centre. Out of these, Austria, Finland and Sweden are Contributing Participants – the status available for non-NATO nations, such as the Republic of Serbia. Australia, Bulgaria, Norway and Switzerland are all in the process of joining. Most recently, Romania and Montenegro also expressed their willingness to join the Centre.

ITU-IMPACT

The International Telecommunications Union (ITU) is the United Nations specialized agency for information and communication technologies. Based on ITU's Global Security Agenda aimed at fostering international cooperation and enhancing confidence and security in the information society, 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, analyse and respond to cyber threats across 193 ITU member states. The partnership is a global multi-stakeholder and public-private alliance against cyber threats, gathering representatives of industry, academia, civil society and international bodies.[132] It 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, it is also active in organizing cyber drills. Serbian representatives from the Regulatory Agency for Electronic Communications and Postal Services (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

131 NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/index.html.

132 ITU-IMPACT. ITU. https://www.itu.int/en/ITU-D/Cyber security/Pages/ITU-IMPACT.aspx.

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 cyberspace[133], 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[134], as well as the accompanying action plan for its implementation, were developed. The Republic of 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.[135]

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 programmatic support in the area of cyber security, provided to developing countries (which have to ask for this assistance from the UN).[136] 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.[137]

In the Western Balkans, this option has thus far been used by Former Yugoslav Republic of Macedonia, where UNDP has already provided support to state institutions in reforms related to the security system within the country's EU accession agenda. Within this framework, special focus has been placed on development of a National Cyber Security Strategy, whereby UNDP has offered assistance in the preparation of a Study on the assessment of conditions for development of a national cyber security strategy. In the area of information technology, the Republic of Serbia is currently using UNDP resources within the open data initiative, implemented in cooperation with the World Bank, as well as digitalization, implemented by the Ministry of State Administration and Local Self-Government.[138]

133 Analysis of Threats in Cyberspace of Montenegro. 2014. Ministry of Information Society and Telecommunications. The Government of Montenegro.

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

135 List of Member States. ITU. https://www.itu.int/online/mm/scripts/gensel8. Countries. IMPACT. http://www.impact-alliance.org/countries/alphabetical-list.html.

136 UNDP Cyber security 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-Cyber security.pdf.

137 Ibid.

138 Open Data: Open Opportunities. 12.1.2016. UNDP in Serbia. http://www.rs.undp.org/content/serbia/sr/home/ourperspective/ourperspectivearticles/otvoreni-podaci--otvorene-mogunosti.html.

Private sector initiatives

With overwhelming recognition of the roles and responsibilities the private sector could and/or should assume in the cyber era, a number of leading global private companies have already established initiatives and programmes of cooperation with national governments. These programmes range from capacity building courses, to provision of products and services, to consultancy support when it comes to developing policies. The rise of such programmes complements the general trend of developing cyber security frameworks through the establishment and strengthening of public-private partnership mechanisms.

Microsoft

Through its European Union Government Affairs (EUGA) department, Microsoft works with EU institutions and partners from industry and civil society to help shape commercially reasonable policies that advance cyber security and enable at the same time the company to pursue its own interests. Within its efforts to cooperate with and support national governments in establishing more cyber-secure frameworks, Microsoft runs the **Government Security Program (GSP)**, aimed at building trust through transparency.

The main goal of the programme is to help governments respond more effectively to computer security incidents, as well as reduce the risk of attacks, deter the attacks themselves, and mitigate exploits. Including over 40 countries and international organizations represented by more than 70 agencies thus far, the GSP enables controlled access to source code, exchange of threat and vulnerability information, engagement on technical content about Microsoft's products and services and access to five globally-distributed Transparency Centers, which are located in the United States, Belgium, Singapore, Brazil, and China. Participation is open to qualifying agencies at no charge. Program criteria include requirements that the GSP participants must be a legal entity of a national government and able to sign an agreement on behalf of that government or be an appropriately recognized international organization.

IBM

Similarly, through its Government and Regulatory Affairs programme, IBM provides worldwide public policy and government relations expertise globally. Working with governments on strategic approaches to key economic, governmental and societal issues through dedicated resources in the Americas, Europe, Africa and Asia, IBM aims at agreeing mutual objectives with its partners pertaining to global consistency and local relevancy.

When it comes to the technological strand of the programme, IBM works with governments to encourage policies that foster innovation, protect intellectual property, and encourage use of technology to address important societal needs. Key focus areas include

encouraging balanced cyber security policies that help secure government and private sector IT infrastructure, while maintaining global competitiveness; enabling collaboration between governments and industry in key technology areas such as high performance computing and nanotechnology; promoting reform of intellectual property laws to improve patent quality and reduce unproductive litigation; supporting initiatives that enhance digital privacy protections while imposing legal safeguards on government access to data; and educating governments about the benefits of cloud computing and data analytics as a means to improve government efficiency and citizen services.

CONCLUSIONS AND RECOMMENDATIONS

With the adoption of the Law on Information Security, complementary bylaws, as well as the first national Strategy for the Development of Information Security and a complementary Action Plan, the Republic of Serbia is definitely making progress towards establishing an overall framework governing cyber security in the country. Given the number of initiatives directly or indirectly linked and dependent on having effective provision of cyber security – such as the process of digitalisation of public affairs and services, or the promotion of the IT sector as a generator of economic growth – it can also be said that there is a slowly developing understanding of the need to pay greater attention to this field. Key actors in this field are also seen as gradually warming up to the notion of public-private cooperation and partnerships in various capacities, although more work needs to be done with actors on both sides of this framework. However, failure to adopt a national Action Plan for the implementation of strategic objectives listed within the Strategy timely suggests that following this initial vigour, the level of proactive positivism quickly deflated, leaving the state of affairs in the normative framework in cyber security in the country at a standstill for almost a year. Hopefully, the recent adoption of the Action Plan will provide new impetus for engagement of all relevant stakeholders in a more responsible and efficient manner in the period ahead.

In addition to completing this framework, it is also necessary to review the existing normative framework, adopting necessary amendments to both the umbrella Law on Information Security, as well as its complementary bylaws. This process should be guided by efforts to remove all inconsistencies and deficiencies mapped during the course of its implementation, as well as genuine understanding of the benefits of full alignment with existing principles, standards and practice, primarily within the European Union. In order to implement adopted amendments, due attention should also be paid to the overall capacities of competent institutions.

Given the pace of development in the field of cyber security, adoption of various frameworks at the regional and global level should be continuously monitored in order to keep national normative frameworks up to date. To this end, the various cooperation and capacity building opportunities offered through these regional and international regimes should also be closely monitored and exploited to the fullest extent if the Republic of Serbia is to establish a strong, comprehensive framework of national cyber security.

Recommendations for further development of the normative, strategic and operational framework of cyber security in the Republic of Serbia can be divided into short, medium and long-term measures, as suggested below.

Short-term

With the recognised gradual rise of awareness among various key actors on the need for establishing more effective frameworks and cooperation in the field of cyber security, a coordinated cross-sector system for information exchange should be established. To this end, procedures for communication, especially in terms of notifications exchanged between the competent ministry and the national CERT should be made as clear and efficient as possible. Generally, the national CERT should be given the jurisdiction to fulfil its key role of being the primary contact point for actors wanting to submit notifications on incidents that took place. The gradual growth in the number of special CERTs established makes this process even more needed in the forthcoming period. Only by including all relevant actors in a comprehensive national framework for information exchange as they arise will allow for a strong national incident response mechanism to be established.

The potential which the Body for Coordination of Information Security Affairs has for establishing expert working groups should be utilised, with special attention dedicated to the possibility of establishing a *permanent* expert multi-stakeholder group, linking all key actors from both the public and private sector. This would enable the fulfilment of strategic objectives pertaining to the institutionalisation of public-private partnership for comprehensive development of information security in the country.

The current lack of clarity in certain legislative provisions in the national normative framework governing information security can be overcome in the short-term by adopting specific guidelines for affected actors. To this end, a competent body - such as the Ministry of Trade, Tourism and Telecommunications, o the Body for Coordination - could bear the responsibility of adopting opinions and recommendations pertaining to specific provisions that determine the obligations of different actors and are currently unclear or vague. Such recommendations would serve as guidelines on how to interpret these normative provisions until needed legislative amendments for improving the current state of affairs are adopted. Given the number of opportunities and possibilities open to the Republic of Serbia for establishing and strengthening its national cyber security framework through utilising its membership and engagement in and with various regional and international regimes and organisations, and its relative underuse of these, awareness raising programmes and campaigns should be considered. To this end, more efficient mechanisms for informing all stakeholders of the opportunities available and providing guidance and support on how to apply and put these to use for capacity building and/or establishing international cooperation channels with peers across the globe should be established.

Medium-term

Within the agreed necessary amendments to the Law on Information Security and its complementary bylaws, the primary objective should be reaching more clarity. In this sense, the normative framework should be amended to clearly define the types of incidents to be reported, establish response procedures and codify channels of communication in case of an incident.

In terms of clarity, the position of the Body for Coordination of Information Security Affairs should also be better established within the normative framework, so as to enable more efficient functioning of the Body in general. In particular, the Body should be provided with more operational independence, if it is to fulfil its central coordinating role within the national cyber security framework.

Programmes for continuous awareness raising and capacity building for all levels of state administration and decision-makers are necessary. Such programmes should include basic policy as well as technical aspects of cyber security, including awareness of the significance, risks and possibilities that the notion of cyber security brings, compliance with principles, standards and norms established by the European Union and other international partners, existing solutions and operational mechanisms as well as practice of inclusion of all relevant actors in all segments. All public officials should possess at least basic knowledge of this field, whereas some categories of civil servants should undergo additional focused training, depending on their specific position, tasks and responsibilities. An opportunity for such government-wide capacity-building programme has been opened by the establishment of the National Academy for Public Administration in 2018.

Frameworks for continuous testing of developed and adopted procedures should be established through the conduct of exercises and drills with the participation of all relevant (affected) actors. This would enable testing adopted procedures in a situation simulating a real life event, and provide feedback and input for potential reviews and amendments of existing normative frameworks.

Existing cooperation channels with international partners should be better utilised, especially within the field of cyber security policy development efforts. This is especially tied with the potential that the Ministry of Foreign Affairs can exploit through establishing sectors or working groups for cyber diplomacy. Additionally, given the country's engagement in existing OSCE and UN mechanisms for confidence building and international regime development efforts, the role of national representatives in working groups focused on these issues should be clearly codified. This relates to the jurisdiction, procedures, freedom and timeframe within which these persons can act, all of which need to be institutionalised.

Within efforts aimed at bridging the gap between the technical and policy-oriented communities working on cyber security, the introduction of multidisciplinary undergraduate and post-graduate teaching programmes at universities should be considered. These courses should, in addition to technical aspects of cyber security, include policy-focused modules, to foster development of future experts capable of bridging the gap between these two communities. As a starting point, introduction of at least optional courses at relevant faculties should be sought, developing later into full study programmes.

Long-term

Given the scope of the field of cyber security, a permanent solution for coordinating efforts and activities of the number of various actors engaged needs to be sought at the national level. To this end, establishing an autonomous governmental body focused solely on cyber security should be considered, which would have a key role in the vertical (through levels of state administration) and horizontal (across actors and sectors) coordination and formulation of policies in this field, maintaining a permanent dialogue and advocating for such issues to be set at the top of the national political agenda. In practice, this can be done in a number of ways, depending on the long-term strategic vision of the Government's composition, held by the Government itself. If the composition of Government, that is, the division of focus areas among competent ministries remains the same, greater proactive focus on cyber security can be provided through amending the legislative framework to allow for greater independence of the Body for Coordination of Information Security, placing it directly under the Government's (Prime Minister's or President's) jurisdiction, for example. If, on the other hand, long-term plans include considering a re-composition of the Government institutions and their focus areas, going as far as establishing a specific Ministry for Cyber security is an option that can be sought. This would bring matters related to cyber security to the first lines of Government focus, and ensure a more proactive and efficient approach to completing and strengthening the national framework in this field, at the same time bearing in mind international obligations.

ABOUT THE PUBLISHERS

Unicom Telecom

Unicom-Telecom is a system integrator company, with a strong focus on developing solutions and services, nurturing a culture of innovation and people development. It was established in 2014 and works in almost all industrial branches – government, telco, finance, utility, retail and SMB - responding to the customer's needs and requirements. The main focus is on cybersecurity, IT infrastructure, business solutions and product development. Unicom Telecom is involved in cybersecurity in Serbia and other countries in the region on various levels – from strategic, policy to technical level – participating in different strategic workgroups and implementing cybersecurity solutions.

Unicom-Systems (subsidiary of Unicom-Telecom) is a registered internet service provider and first registered commercial CERT in Republic of Serbia. Its UniCERT team provides holistic security services – based on best-of-the-breed technologies, always available (24/7) operational team and experienced expert team – from protection and detection to incident response. The service portfolio includes unique antimalware scrubbing center featuring Endpoint Detection and Response, Application and Infrastructure Protection, Network and Email Security, Information Protection and custom SOC Services – Cybersecurity Monitoring and Detection, Incident Response, Audits, PenTests and Trainings (Expert Trainings, Awareness Building, Cybersecurity Exercises)

IBM

IBM Security solutions and services integrate new and existing security capabilities across domains. This delivers critical visibility, provides comprehensive controls and helps reduce complexity.IBM expertise stems from more than 6,000 hands-on professionals and researchers supporting customers in more than 130 countries. Our deep insight comes from monitoring more than 270 million endpoints and managing 15 billion events each day and is built into IBM products and services, provided via real-time client feeds and embedded in professional engagements. We're committed through research and development investment, hiring and retaining the best talent, and extensive thought leadership to helping you safeguard your organisation. Our new approach to security can enable organisations to innovate while reducing risk. We can provide you a pathway for growing your business while helping secure your most critical data and processes.

Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide.

Juniper builds stronger, more secure and trusted networks, thanks to a security portfolio that delivers end-to-end protection from attacks across every environment—from the data center to campus and branch environments to the device itself. Our extensive experience in developing security software and high-performance scalable systems for the service provider market is what makes Juniper Networks a valuable partner in securing new technologies that require new approaches.

ANNEX I: Members of the Petnica Group

The Petnica Group includes representatives of:

- Association of Serbian Banks
- Faculty of Organisation Sciences of the Belgrade University
- Faculty of Security of the Belgrade University
- General Secretariat of the Serbian Government
- Government's Office of Information Technologies and e-Governance (which hosts the govCERT)
- Innovation Fund
- Microsoft Serbia
- Military Security Agency
- Ministry of Defence
- Ministry of Foreign Affairs
- Ministry of Interior
- Ministry of Trade Tourism and Telecommunication (competent ministry for cyber security)
- Office of the National Security Council and Classified Information Protection (NSA)
- Office of the Prosecutor for High Technology Crime
- Regulatory Agency for Electronic Communications and Postal Services (which hosts the nCERT)
- SHARE Foundation
- Security-Intelligence Agency
- Serbian National Internet Domain Registry
- Telekom Serbia
- Telenor Serbia
- Unicom Telecom
- Vip Mobile
- independent experts

Representatives of the Republic of Serbia in both the OSCE Informal Working Group on Cyber Security as well as the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security are among its members.

ANNEX II: Cyber Drill Report

The first national policy-related cyber drill, which took place in late 2017, aimed at supporting the further strengthening of a comprehensive national framework of cyber security being established in the Republic of Serbia. Focusing on existing capacities and jurisdictions, as well as procedures and frameworks regulating communication and cooperation, based on a realistic, tailor-made scenario of a national cyber incident, the drill enabled:

– Analysing and determining the level of efficiency and applicability of existing procedures in case of a national cyber incident in a realistic framework;

– Mapping existing mechanisms for communication and cooperation between key actors in case of a national cyber incident, highlighting potential vulnerabilities (snapshot of the current situation);

– Showcasing the need for mutual cooperation of public institutions in case of a national cyber incident and recommending solutions for the development of such a mechanism;

– Providing specific recommendations for strengthening the structures for communication and cooperation among key national actors, both public and private, in the case of a national cyber incident;

– Contributing to strengthened coordination among key public and private actors in case of a national cyber incident, encouraging better operative cooperation, supporting thus the entire national cyber security framework;

– Raising the level of awareness of public and private actors on their mutual operative roles, responsibilities and capacities in case of a national cyber incident;

– Clarifying procedures for communication with key international organisations dealing with cyber security on identified incidents (e.g. OSCE's Informal Working Group on Cyber security, UN's ITU, various EU bodies and CERT associations);

– Supporting the competent ministry (Ministry of Trade, Tourism and Telecommunications) in further developing the national cyber security framework by providing concrete and factual recommendations focused on crisis management and incident response mechanisms, adapted to the national framework and taking into account international best practice examples.

The drill, that is, its scenario and wider concept, was primarily developed by Irina Rizmal, acting as a consultant engaged by DiploFoundation specifically for the needs of the exercise; Vladimir Radunović, Director of the cyber security and eDiplomacy programme at DiploFoundation; and Adel Abusara, Senior Project Assistant at the OSCE Mission to Serbia. In terms of context and aims, the drill scenario was additionally cross-checked with foreign experts, namely, Gorazd Božič, Director of Slovenia's nCERT (SI-CERT) and Stefanie Frey, Director of Deutor Cyber Security Solutions, previously a coordinator for the implementation of the National Cyber Strategy of Switzerland at the Swiss Government. Technical possibilities of the envisioned incident were reviewed with representatives of IBM in the Republic of Serbia.

Additionally, the drill relied on preparatory activities carried out in the form of a consultative workshop in early 2017, within a project implemented by the Geneva Centre for Democratic Control of Armed Forces (DCAF) with the Ministry of Interior of the Republic of Serbia. At this workshop, representatives of competent public institutions and bodies developed draft communication procedures later submitted for consideration to the Body for Coordination of Information Security Affairs.

The drill itself was based on a tailor-made scenario. It envisioned a situation in which a serious national cyber incident takes place, escalating through several phases. It was primarily focused on crisis communication procedures in terms of:

– Crisis management

– Reaction and response to incidents

– Normative framework and mandates/jurisdiction

– Existing and/or needed procedures

– Public-private cooperation.

Due attention was dedicated to having the scenario and the entire drill focused primarily to issues pertaining directly to matters of cyber security, with minimal overlap with other risks stemming from cyberspace, such as cybercrime. „Cataclysmic scenarios" with large-scale consequences were also avoided as the authors of the drill considered that its main goal – testing crisis situation communication procedures – can be equally achieved by simulating smaller – yet comprehensive – national cyber incidents. For this reason, the drill avoided, for example, cyber-attacks on critical infrastructure or non-nuclear infrastructure such as the electric grid, as is the common pattern.

The drill was designed to enable all participants to take part from equal and neutral positions meaning they did not represent the official positions of their institutions/organisations, but were encouraged to highlight to what extent are the recommended, potential solutions realistic and applicable from the point of view of their respective institutions/organisations. Recommended solutions were therefore not limited by existing procedures and practice, but took into account existing capacities in terms of human, technical and procedural resources in the Republic of Serbia.

Twenty-nine participants were divided into five working groups with balanced representations of the public and private sector actors in each group. Represented institutions and organisations differed in each group, which contributed to differing formats of the solutions suggested. One moderator was allocated to each working group, charged with leading the discussion following a number of predetermined questions of interest as a basis. Each working group also nominated a rapporteur, tasked with presenting key conclusions of the group discussion, aimed at highlighting good practice examples and possible solutions, as well as spotted obstacles and challenges for establishing efficient inter-sectoral communication channels. Participants were also asked to, within their working groups, define three greatest challenges and/or important conclusions that should find their place in the final Drill Report. Following presentations of each working group, participants considered the presented results, conclusions and recommendations together, in order to define most common trends and challenges, as well as the most realistic solutions among those suggested.

Upon completion of the drill, the group moderators summarised all the information gathered throughout its course, as well as the closing discussion, designing thus the basis of a final Drill Report. The Report thus provided a factual overview of the current state of affairs in cyber security in the Republic of Serbia, as well as specific recommendations for its further development. The aim of the Report was to introduce key decision makers with the burning problems that actors in this field are faced with, but also to provide clear, fact-based, plausible solutions for some of the possible challenges in the process of developing crisis situation communication procedures. As such, the Report posed as a pioneer document presenting joint conclusions and suggested solutions of the public and private sector for developing cyberspace crisis situation procedures in the Republic of Serbia.

Developed recommendations have been divided into several thematic areas, as follows.

Recommendations related to prevention

Given the normative principle of risk management, as well as the limited capacities among ICT operators of essential services, it is necessary to establish a mechanism that would enable fulfilment of this principle in an adequate manner. To this end, one suggestion was to *establish a body tasked with supporting ICT operators of essential services in the process of risk assessment*, in line with legal obligations. An alternative solution is to have this task delegated to envisioned inspectors for information security, as according to the Law on Inspection Supervision, this body is to have both an educational and preventive role. The greatest current obstacle for such a solution are the limited capacities of the Ministry of Trade, Tourism and Telecommunications, which should encompass this service.

The need for a *coordinated system comprising several institutions for exchange of information of importance for incident prevention* has also been highlighted. The functioning of this system would include, among other, monitoring of online content, social networks as well as other intelligence data from different sources available to public bodies and the private sector. By cross-referencing such information, a national system of prevention would be stronger and more efficient.

Recommendations related to operative challenges

Codification of communication channels and responsible persons in key actors of the national cyber security framework is necessary. The first step would be to develop and implement standard operating procedures for crisis communication in case of an incident in national cyberspace. Existence of such formal procedures further requires establishing official contact points in all institutions and organisations within the national framework.

All channels of communication need to be two-way, otherwise they will not be efficient as there will be no genuine exchange of information.

It is necessary for the Body for Coordination to have an up-to-date *contact base* of operators, providers and financial sector actors in order to ensure that representatives within the Body know who they should contact in case of an incident.

Adopted procedures, as well as those still under development, should be further *tested through simulations and drills* that enable experience, knowledge and information exchange on capacities, in order to enable further development of a communication frameworks that is efficient and plausible, that is, in line with existing capacities. Such drills should include representatives of both the public and private sector, as well as academia and civil society and, if needed, representatives of the media.

Recommendations related to capacities

It is necessary to strengthen operative capacities of the nCERT in order for it to be able to genuinely assume responsibility for legally prescribed activities and build trust among partners through efficient and useful action in practice. A functional nCERT, contributing to the security of other actors through the information it provides, would strengthen trust and interest for operational cooperation, as well as timely delivery of complete information and reports.

Due to limited capacities of the public sector to build a comprehensive national cyber security framework, it is necessary to also *engage the capacities of the private sector*, such as telecom operators and internet service providers who possess the technical abilities to provide support in resolving/analysing an incident and forming recommendations.

In addition, equally targeting both the public and private sector, a key recommendation primarily aimed at the private sector is *fostering the establishment of guild CERTs for more efficient horizontal communication* towards and among all relevant actors in a specific line of work.

By establishing a CERT of telecom operators or internet service providers, an efficient channel of communication towards all actors in this line of work would be established, replacing the current situation in which larger operators are relied on to pass the message to smaller ones. This would reduce the timespan needed for informing all actors, independent of their size, but also ensure that they receive important information through direct channels of communication and be able to act immediately if needed.

Alongside existing informal good practice examples of cooperation among banks through the Association of Serbian Banks with the Department of High-Tech Crime of the Ministry of Interior, an official CERT of banks and other financial institutions would enable more efficient communication directly towards the national CERT, instead of the current situation in which the National Bank of Serbia is relied on as the key hub for information and communication between these two sides.

Recommendations related to the normative framework

In terms of necessary amendments of the normative framework, it is necessary to *determine clear criteria for incident classification* in order to avoid the risk of wrong classification caused by overlapping/differing interpretation of the listed types of incidents. It is necessary to *better define incidents that are to be reported* in order to avoid the risk of having an incident, due to ambiguities in the normative framework, being reported late or going unreported overall. It is also necessary to *review the list of defined ICT operators of essential services* in order to determine the 'criticality' of the listed actors and include those currently left out that could contribute to more efficient response in case of incidents, such as Serbia's Internet Exchange Point (SoX).

In terms of more efficient communication in case of an incident, it is necessary to *include the National Bank of Serbia (NBS)* in the working of the Body for Coordination of Information Security Affairs. The NBS should also be obliged to report incidents and submit all information received to the national CERT. Such communication can be established at the level of a CERT of financial institutions.

A key recommendation is the *need for determining the possibility of establishing a crisis headquarters in case of a cyber incident of national proportion*. Establishing a central operative body, in the form of a crisis headquarters, should be defined by standard operative procedures. A crisis headquarters should be established at government level and gather representatives of the Body for Coordination, representatives of other relevant public institutions, as well as representatives of critical infrastructure – operators, banks and the like.

In order to ensure efficiency of operations of such a body, a narrower composition can be determined to act as an operational team with special powers that can, in case of a national cyber incident, coordinate communication between key actors, issue precise orders, analyses and situational reports, with a direct communication channel with the Prime Minister and/or President. Whether the Body for Coordination, with its current advisory role, could be transformed into a body with an operational role, or another model should be sought remains an open question.

One suggested modality for establishing such an inter-operational body is found in existing practice in the case of the migrant crisis whereby the Government of the Republic of Serbia has the powers to establish special standing inter-operative bodies (working groups), consisting of representatives of relevant institutions. Faced with the migrant crisis, the Government of the Republic of Serbia established a working group to solve the problem of mixed migration flows, which included various public institutions.

If there is intelligence, confidential or secret information that is exchanged, then representatives of ICT operators of essential services and the private sector taking part in the operations of such a body need to be certified. However, given that certification of civilians is a relatively slow process, in order to avoid postponing the establishment of operative capabilities for incident response, a possible solution would be to have competent security services synthesizing all available information, and carry the responsibility for assessing the gravity of an incident and adequate reactions.

In terms of complementarity of the entire normative framework, the need for complete alignment of the Law on Information Security, Law on Personal Data Protection, Law on Data Secrecy and other relevant normative acts has been highlighted.

Recommendations related to communication with the public

It is necessary to *determine clear procedures for communication with the public depending on the type and scope of incidents*. For smaller incidents, template statements are needed. For incidents of greater scope, it is necessary to determine procedures for drafting a coordinated statement, primarily by the competent Ministry and the national CERT, in coordination with the affected actor (e.g. operator or financial institution). A situation in which the nCERT waits for approval and/or directive from the competent Ministry to issue a public statement should be avoided. Template statements can be issued jointly, being published on official websites of both institutions. For incidents of greater severity, a specified competent person is needed to deliver the statement and, if needed, provide additional information and instructions to the wider public, coordinated among all relevant institutions and actors. The message needs to be clear and issued by one delegated source, or several previously determined and coordinated representatives of relevant institutions in order to avoid discrepancies in the message sent by various public bodies. In this way, efficient communication is ensured while preventing potential spread of panic among citizens.

Recommendations related to international cooperation

It is necessary to *determine the competences of representatives of the Republic of Serbia who are contact points for cooperation with international organisations*. These contact points need to be, at the same time, members of the Body for Coordination, and have jurisdiction to communicate with their peers from other states within a prescribed timeframe. Clear procedures should define how and when they react. Contact points need to be institutionalised.

Although the current normative framework does not envision a national contact point for issues pertaining to cyber security, such a solution can be adopted in the forthcoming process of amending the Law on Information Security, in line with the EU Directive on Security of Network and Information Systems (NIS Directive) which prescribes such a form for all Member States. The Directive underlines that such a framework is not necessarily

expected from "third countries", but that they *can* establish it. Given the strategic priority of the Republic of Serbia to become an EU Member State, there is no reason why it cannot already start work on alignment with EU principles in this field by establishing a body and/or nominating a representative that would have the role of a national contact point for cyber security (acting as a liaison officer), directly accountable to the Prime Minister. The Body for Coordination of Information Security Affairs could use this point as its main channel for communication towards the Prime Minister and/or President, or itself be given the role of a national contact point within the forthcoming amendments of the existing normative framework.

Given that the national CERT is currently listed only within the Trusted Introducer[139] platform for support to activities of Computer Emergency Response Teams in case the security of information systems is jeopardised, as it does not fulfil the conditions for membership in the First[140] platform, nor is it a member of the European Network and Information Security Agency (ENISA; as it is not an EU Member State), the government can once again partially *rely on private sector capacities*. Namely, different private sector CERTs, such as CERT of financial institutions can be (and already are) members of guild international networks through which information of interest – in case of a national cyber incident – can also be obtained.

The need for greater involvement of the Ministry of Foreign Affairs in matters pertaining to international cooperation in the field of cyber security and development of mechanisms for participation in national coordination in case of cyber incidents has also been recognised.

Recommendations related to inspection and reporting

In order for the national CERT, in accordance with the Law, to be in a position to carry out detailed analysis of incidents and develop reports containing recommendations following an incident, *exchange of information on conducted inspections in relevant institutions and organisation is necessary*, including both the public and private sector. This is why it is necessary to define an obligation of the National Bank of Serbia, as well as other actors such as telecom operators and Internet Service Providers, to submit reports on conducted inspection supervision. As these reports can contain sensitive data related to ongoing investigations (if, for example, the High-Tech Crime Department of the Ministry of Interior or the Prosecutor's Office are launching an investigation), as well as sensitive information for the functioning of operators and providers, it is necessary to determine procedures for submission of these reports in an anonymised format.

One suggested solution is to have reports on inspections conducted within other institutions and organisations delivered to the competent Ministry which would filter out

139 Support network for CERTs counting over 150 world CERTs from different fields of work. Trusted Introducer. https://www.trusted-introducer.org/index.html.

140 Network of CERT teams counting over 300 members from Africa, America, Asia, Europe and Oceania. FiRST. https://www.first.org/.

information on *who* has been affected, leaving only technical information and forwarding such anonymized information to the nCERT. If the competent Ministry lacks the capacities for this, an alternative solution is to establish a working group within the Body for Coordination of Information Security for this purpose, which is in accordance with the Law. In this case, the Body for Coordination should be tasked with compiling a report on incidents that have repercussions for national security and issue recommendations.

In terms of *recommendations* coming out of such reports, these have to be developed based on the current state of affairs and capacities, and be time-limited. One question that remains open is who should be tasked with reviewing whether these recommendations have actually been implemented in general, and in accordance with the prescribed timeframe. This is a challenge especially when it comes to the private sector.

Institutions and organisations that took part in the drill:

- Association of Serbian Banks
- Banca Intesa
- General Secretariat of the Government of the Republic of Serbia
- Microsoft Serbia
- Military Security Agency
- Ministry of Defence
- Ministry of Foreign Affairs
- Ministry of Interior
- Ministry of Trade, Tourism and Telecommunications
- National Bank of Serbia
- national CERT/Regulatory Agency for Telecommunications
- Office of the National Security Council and Classified Information Protection
- Prime Minister's Chief of Staff
- SHARE Foundation
- Security Intelligence Agency
- Telecom Serbia
- Unicom Telecom
- Vip Mobile