Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities

Research report under the project
"Cybersecurity Capacity Building and Research Programme for South-Eastern Europe"
implemented with the support of the Federal Department of Foreign Affairs of Switzerland

Authors:
Ms Adriana Minović, Digital Watch at the Geneva Internet Platform
Mr Adel Abusara, OSCE Mission to Serbia
Ms ErandaBegaj, Institute for Democracy and Mediation, Albania
Mr Vladimir Erceg, Belgrade Centre for Security Policy, Serbia
Mr Predrag Tasevski, Founder of CyberSecurity.mk
Mr Vladimir Radunović, DiploFoundation
Ms Franziska Klopfer, the Geneva Centre for Democratic Control of Armed Forces (DCAF)

DiploFoundation, Geneva
September 2016

Contents

1 Introduction 4

2 Research background, methodology and outline 6

3 Overview of the relevant European and international legal environment 8

3.1 The Council of Europe's legal instruments 8
3.2 European Union (EU) legislation 9
3.2.1 Strategic Documents at EU level 9
3.2.2 Secondary Legislation at the EU level 11
3.3 International Soft Law 12

4 State of play in the Western Balkans 15

4.1 Albania 15
4.2 Bosnia and Herzegovina 16
4.3 Croatia 17
4.4 Kosovo* 18
4.5 Montenegro 19
4.6 Republic of Macedonia 20
4.7 Serbia 21
4.8 Regional summary 22

5 Activities and support instruments of international organisations in the Western Balkans 24

5.1 The European Union (EU) and the Council of Europe (CoE) 24
5.2 The North Atlantic Treaty Organisation (NATO) 27
5.3 The United Nations Development Programme (UNDP) 29
5.4 The Organisation for Security and Cooperation in Europe (OSCE) 30
5.5 The International Telecommunication Union (ITU) 31

6 Existing regional security mechanisms and opportunities 34

6.1 The South-East European Cooperation Process (SEECP) 34
6.2 The South-East European Cooperation Process Parliamentary Assembly (SEECP PA) 35
6.3 The Regional Cooperation Council (RCC) 36
6.4 The South-East European National Security Authorities (SEENSA) 37
6.5 The South-East European Military Intelligence Chiefs (SEEMIC) 38
6.6 The e-SEE Initiative 38
6.7 The Centre for Security Cooperation (RACVIAC) 39
6.8 The South-East Europe Cyber Security Centre (SEECSC) 39
6.9 The Southeast European Law Enforcement Center (SELEC) 40
6.10 The South-East European Prosecutors Advisory Group (SEEPAG) 41
6.11 The Southeast Europe Police Chiefs Association (SEPCA) 41
6.12 Police Cooperation Convention for Southeast Europe (PCC SEE) 42
6.13 The Regional School of Public Administration (ReSPA) 42
6.14 The Central European Initiative (CEI) 42
6.15 The South-Eastern Europe Defence Ministerial Process (SEDM) 43
6.16 Projects relevant for the Western Balkans 43

7 Conclusion 45
8 Recommendations 51
8.1 Recommendations for the Western Balkans countries 51
8.2 Recommendations for International Organisations 52
8.3 Recommendations for regional cooperation 53
8.3.1 Enhancing regional cooperation through existing institutions 53
8.3.2 Enhancing regional cooperation through the creation of a regional cybersecurity centre of excellence 55
About the authors 57
About DiploFoundation 59

1 Introduction

Cyberspace has become an essential component of modern society. Critical societal infrastructure, the financial sector, governmental services, the security sector, schools, and hospitals are increasingly and irreversibly dependent on interconnectivity and the global network. So are our citizens. The merits of the open Internet are accompanied by risks.

While national cybersecurity policies are bound by the borders of national sovereignty, the physical cybersecurity sphere (infrastructure, equipment, logistics) and its logic disregard these borders, becoming an international issue. For this very reason, no country can achieve an acceptable level of cybersecurity on its own, which makes it paramount to address the myriad of cybersecurity-related issues through regional and international cooperation.

On the other hand, the threats are differing, with new ones arising every day with various actors included, either as part of the problem or the solution. Having said that, it is not surprising that measures to address the threats come from different areas: political, economic, technological, legal, managerial or military. All these measures need to come together to offer sustainable and complying solutions to strengthen security in the cyber-sphere. Also, it is of utmost importance to ensure that any security measures foreseen are consistently balanced against rights and freedoms, which is again safeguarded by the legal framework created on the international level. In all these efforts, dialogue and cooperation with the private and civil sectors is crucial for the efficiency of policy and operative approaches.

Cyberspace is an intrinsic part of the development of any country. A strong information and cyber capacity is crucial for the region to progress and develop in the economic, political and social spheres.[1] The exponential growth of devices connected to the Internet and "netizens" (active Internet users) will mostly take place in emerging economies. Social and cultural benefits of cyberspace will be immense for those countries – "The growth of cyberspace helps close the digital divide between the rich and the poor. By boosting the number of 'digital natives' it offers many new opportunities for advancing human development".[2] Yet, greater reliance on cyberspace introduces many new risks and vulnerabilities. The ever-increasing threat of cyber-attacks will affect developing countries on several levels: their critical (information) infrastructure will be particularly vulnerable; their nascent digital economies might crash if systematically attacked; widespread fraud without fast state response might deter participants from using e-commerce. It is therefore of utmost importance for all countries - especiallythe developing ones - to create a legislative and strategic framework and institutions that are sustainable and solid enough to be able to implement this framework, both on technical and policy-based level.

Many countries have adopted national cybersecurity strategies and related legislation, taking into account both security and freedoms. A growing number of countries have set up national mechanisms for response to cyber-incidents, involving government as well as the corporate, academic, and NGO sectors. Some have declared 'cyber' as the fifth military domain, and have set up

[1]Lilly Pijnenburg Muller , "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities" Report no. 3, 2015, Norwegian Institute of International Affairs, available at:https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf

[2]Magdy Martinez-Soliman, Deputy Assistant Administrator, UNDP, Seoul Conference on Cyberspace, October 2013, available at: http://www.undp.org/content/seoul_policy_center/en/home/presscenter/articles/2013/10/18/-seoul-framework-could-make-cyberspace-safer-more-accessible-.html

defensive and offensive cyber-commands within their armies. South-Eastern Europe, and especially the Western Balkans, is lagging behind.

The region, however, is not immune to these risks. With the increasing digitalisation of society, including emerging e-government services and databases, interconnecting the critical infrastructure and industry, and enhancing online banking and financial services, the stakes are growing sky-high. A country-scale cyber-attack of one country in the Western Balkans could result in a direct loss of more than €10 million per day[3]. Numerous smaller-scale incidents were recorded in the Western Balkans in previous years, while it remains possible that large-scale ones - such as the Advanced Persistent Threat (APT) attacks with malicious code inserted in critical systems leaking data or being dormant until the attackers trigger it to perform a possibly devastating attack - are also present but there is no mechanism to detect and report them. Most countries of the Western Balkans, however, do not have efficient institutional mechanisms – operational or legislative – for risk assessment, information sharing, prevention, and quick incident response. This comes primarily as a result of the lack of political awareness of the problem and institutional capacities to recognise the risk and act upon it in a cooperative manner on the regional level.

[3]Radunović V (2013) DDoS - Available Weapon of Mass Disruption.*Proceedings of the 21st Telecommunications Forum (TELFOR)*, pp.5-9. Available at: http://www.diplomacy.edu/resources/general/ddos-available-weapon-mass-disruption

2 Research background, methodology and outline

In 2014, the “Young Faces Network Cybersecurity Winter School for the Western Balkans and Moldova”, organised by the Geneva Centre for Democratic Control of Armed Forces (DCAF) and DiploFoundation (Diplo), enhanced the knowledge and created a community of 30 young cybersecurity professionals from the region. The direct and indirect outcomes of the Cybersecurity Winter School were several follow-up activities in the region, including the project "Cybersecurity Capacity Building and Research Programme for South-Eastern Europe", conducted from December 2015 to May 2016 by Diplo and the DCAF, with the support of the Federal Department of Foreign Affairs (FDFA) of Switzerland. The project consisted of an online course in cybersecurity policy for 30 youth officials and professionals from the SEE, and the research work exploring policy and cooperation gaps in the Western Balkans. It contributed to increasing the capacities of public institutions, as well as the private sector and civil society in South-Eastern Europe (SEE) and particularly in the Western Balkans, to respond to growing cybersecurity challenges that impact national security, rights and economic growth.

This report is the result of the research phase, which aimed at analysing policy-related gaps and mapping the existing institutional frameworks in the Western Balkans, in order to enable further discussion on addressing the existing gaps through enhanced cooperation and investments in the region. It was conducted between February and May 2016 by a group of 5 researchers, selected among the successful participants of the Cybersecurity Winter School, accompanied by the two experts from Diplo and the DCAF.

The methodology was based mainly on desk research, combining a review of international and regional legislation relevant for the region, content analysis and secondary analysis of the already available regional or global reports that provide certain information about cybersecurity policy levels in the countries of the Western Balkans, enquiries of policy developments in each of the countries, and a final analysis to draw conclusions and suggest recommendations.

The report starts with the overview of international and European legal environments; it does not, however, present a comprehensive review of global legal mechanisms but focuses on those relevant for the Western Balkan countries due to their geopolitical tendencies.A study of the state of affairs in the region and particularly the policy gaps is then provided, with a short profile of each of the seven countries/territories - namely Albania, Bosnia and Herzegovina, Croatia, Kosovo*[4], Montenegro, the Republic of Macedonia and the Republic of Serbia - and a brief regional “zoom-out”. A mapping of the existing security cooperation mechanisms in the region follows, in order to identify gaps in and potentials for cybersecurity cooperation. A review of major projects and funding opportunities in cybersecurity in the Western Balkans by major international organisations is presented afterwards. A comprehensive conclusion is accompanied with recommendations for the possible next steps towards improving the state of play in theWestern Balkans countries, a more systematic regional approach by international organisations, and enhancing regional cooperation.

Due to the nature of the research field, the number of terms and titles of the organisations are continuously abbreviated, keeping the full format in the first appearance. The geographical term

[4]Used according to the "asterisk agreement" from 24 February 2012, the asterisk stands for: "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".

Western Balkans is used to denote the group of seven countries listed above, and is sometimes replaced by the abbreviation *WB*. In addition, even though there are different understandings of the terms cybersecurity and information security, in this report both terms are understood equally and used successively,often in the abbreviated forms as CS, IS or CS/IS. Similarly, the terms CERT, CIRT and CSIRT are used interchangeably, yet always referring to the same: the team for response to cyber-incidents.

The report is seen as a building block in the broader regional endeavour, which started with the Winter School in 2014. It should serve to discuss further in-depth research on the regional and national levels, possible follow-up projects that could initiate discussions on ways to develop comprehensive national developments, enhance regional cooperation and increase institutional capacities in cybersecurity.

The illustrated executive summary is available at: www.diplomacy.edu/cybersecurity.

3 Overview of the relevant European and international legal environment

A legal framework is the starting point for mapping cooperation in a respective area. Through the adoption of conventions, declarations and transposition of other legal acts, the countries are taking a common approach in certain areas, thus recognising the need for cooperation where more work is needed. In regards to the Western Balkan countries, the EU is the main umbrella that has a comprehensive legal framework in the field of CS/IS, which the Western Balkan countries are adopting in the process of the EU accession. Beside the EU, there are other international organisations that also influence the work of the Western Balkan countries in this field, such as the Council of Europe (CoE), Organization for Security and Cooperation in Europe (OSCE) and others. In this chapter we will map the most important documents constructing the legal framework in the CS/IS relevant to the Western Balkans countries.

3.1 The Council of Europe's legal instruments

The most important international convention in the area of cybersecurity is the 2001 **CoE Convention on Cybercrime (also called the Budapest Convention)[5].** The CoE Convention is a legal framework of reference for combating cybercrime, including attacks against information systems. This convention, supplemented by the Protocol on Xenophobia and Racism Committed through Computer Systems, is the only binding international agreement related to cybersecurity, and is considered an archetypal template for countries to use domestically. The Convention is signed by 54 countries(ratified by 48) from around the world and all the Western Balkan countries are part of the convention.

The Budapest Convention requires parties: to adopt appropriate legislation against cybercrime; ensure adequate procedural tools to effectively investigate and prosecute cybercrime offenses; and to provide international co-operation to other parties engaged in such efforts. The Budapest Convention thus introduces:

a) Common standards (achieved through national legal measures such as the criminalisation of the above mentioned offences).
b) Capacity building (the Cybercrime Programme Office is established on the basis of the standards of the Budapest Convention, in order to assist countries worldwide in strengthening their legal systems' capacity to respond to the challenges posed by cybercrime and electronic evidence).
c) Technical cooperation (extradition, mutual assistance, spontaneous information).

The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) (also called the Lanzarote Convention)[6]represents the most advanced and comprehensive standard in this field. The Lanzarote Convention has been signed and ratified by 40 states including all Western Balkans countries.

The importance of the Lanzarote Convention in this case is that it contains many references to the use of information and communication technologies in the context of sexual exploitation and sexual

[5]CoE, Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185
[6]Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse * Lanzarote, 25.X.2007,Council of Europe Treaty Series - No. 201

abuse of children. For example, it requires states to criminalise conduct such as knowingly accessing child pornography on the Internet. This treaty and the Convention on Cybercrime thus complement each other.

Also, although it is not one of the core problems of CS/IS, the transfer of personal data and data protection issues are related to this field in a significant manner. It is therefore worth mentioning that **the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS no.108)**[7]is signed by 47 states, including Western Balkan countries. The objective of this convention is to strengthen data protection and the legal protection of individuals with regard to the automatic processing of personal information relating to them. The importance of this convention isparamount, especially having in mind the need for legal provisions of the so-called e-government. The Convention provides a mechanism of cooperation and sets clear rules in regard to the cross border transfer of data, introduced in signatory countries through respective state bodies in charge of Data Protection. However, in light of the soon-to-be annulled Directive on data protection[8], the EU-US Privacy Shield Framework issues and the introduction of a new set of rules on data protection in Europe, it is evident that even the EU countries are starting to take new approach in a still untested field, which will increase challenges for implementation.

3.2 European Union (EU) legislation

The EU integration, as the most significant project and strategic goal of all Western Balkans countries, is the most effective mechanism for the harmonisation of legislation and enhancement of cooperation among the countries embarking on this process. The Stabilisation and Association Agreements, as the main documents related to the EU enlargement process, *inter alia* foreseen obligations for all the Western Balkan countries to align their national legislation with EU *acquis.*. The main pieces of EU legislation in force in the area of CS/IS relevant for the Western Balkan countries are therefore analysed below.

3.2.1 Strategic Documents at EU level

The Digital Agenda for Europe (DAE), adopted in May 2010[9], is one of the most important strategic documents on the EU level that highlighted the shared understanding that trust and security are fundamental preconditions for the wide uptake of ICT and achieving the objectives of the 'smart growth' dimension of the Europe 2020 Strategy. Under its Trust and Security chapter, the DAE emphasised the need for all stakeholders to join forces in a holistic effort to ensure the security and resilience of ICT infrastructure, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated security mechanisms. In particular, key action 6 of the Digital Agenda for Europe calls for measures aimed at reinforced and high-level Network and Information Society policy.

In order to catch up with the additional technical innovations and policy challenges emerging in the years of the development and adoption of the DAE, the **Digital Single Market Strategy for Europe**[10]was adopted in May 2015,creating thefirst industry-related initiative**.** For new connecting

[7]CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981

[8]Namely, the General Data Protection Regulation (Regulation (EU) 2016/679), which was adopted on 27 April 2016 will replace the current data protection directive (officially Directive 95/46/EC) when it enters into application on 25 May 2018.

[9]Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions A Digital Agenda For Europe, /* Com/2010/0245 F/2 */

[10]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, Com (2015) 192 Final

technologies to take off, EU countries' citizens need to have confidence in them, which is why trust and security are at the core of this strategy. The Digital Single Market Strategy is built on three pillars: better access to digital goods; an environment for digital networks and services to flourish; and maximising the growth of the digital economy. In order to accomplish the given goals, the European Commission proposes concrete measures[11] to speed up the standard setting process, including focusing on cybersecurity, among others.

Following new competencies conferred on the EU institutions by the Treaty of Lisbon, the**EU Cybersecurity Strategy** was adopted in 2013[12]. The Cybersecurity Strategy is the EU's first comprehensive policy document in this area. Its five strategic priorities are clear:

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing a cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Developing the industrial and technological resources for cybersecurity
- Establishing a coherent international cyberspace policy for the EU and the promotion of core EU values.

Furthermore, as a result of new developments in this field and as an attempt to react to terrorist attacks in the EU, **The European Agenda on Security (EAS)[13]** was approved in 2015, providing the overall strategic framework for the EU initiatives on cybersecurity and cybercrime. The Agenda envisages reinforcing the capacities of law enforcement authorities, in particular through the Europol's European Cybercrime Centre, and addressing the obstacles to criminal investigations on cybercrime, notably in relation to access to evidence. Key actions under this Agenda include[14], among others, updating the Framework Decision on Terrorism[15], enhancing dialogues with the IT industry, and reinforcing tools to fight cybercrime. It also highlights the importance of enhancing the capacities of Europol,including the creation of the European Counter Terrorism Centre which will help the Europol step up support for national law enforcement authorities' actions to tackle foreign terrorist fighters, terrorist financing, violent extremist content online, and illicit trafficking of firearms.

With respect to the development of cyber defence capabilities,**the EU Cyber Defence Policy Framework** approved in 2014[16] is one of the main documents that specifically address these issues. It serves as groundwork for countering threats arising from cyberspace and it specifies five priority areas for Common Security and Defence Policy (CSDP) cyber defence:

1. Supporting the development of Member States' cyber defence capabilities related to CSDP;
2. Enhancing the protection of CSDP communication networks used by EU entities;

[11] Available at: https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market

[12] Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, Join(2013) 1 Final.

[13] 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, Com(2015) 185 Final

[14] European Commission - Press release, "Commission takes steps to strengthen EU cooperation in the fight against terrorism, organised crime and cybercrime, Strasbourg", 28 April 2015, available at: http://europa.eu/rapid/press-release_IP-15-4865_en.htm

[15] Council Framework Decision of 13 June 2002 on combating terrorism, Official Journal L 164 , 22/06/2002 P. 0003 - 0007, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002F0475

[16] EU Cyber Defence Policy Framework as adopted by the Council on 18 November 2014, 15585/14.

3. Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector;
4. Improving training, education and joint exercise opportunities;
5. Enhancing cooperation with relevant international partners, particularly NATO.

On the other hand, it is worth mentioning that the **European Strategy for a Better Internet for Children**[17] aims to establish a safe online environment to give children the digital skills and tools they need to fully and safely benefit from being online.

3.2.2 Secondary Legislation at the EU level

The directive on network and information security (NIS)[18]**,** entering into force in August 2016[19], requires each member state to establish a Computer Security Incident Response Team (CSIRT) and a competent national authority for NIS, and sets up a cross-EU cooperation group for strategic cooperation as well as a CSIRT Network for operational cooperation, among other provisions. The directive also ensures that information is shared between the private and public sectors, and defines several categories of operators of essential services which are required to take appropriate security measures and notify the relevant national authorities of serious incidents; these include operators in sectors of energy, transport, banking, financial market infrastructures, health, water, and digital infrastructure (including Internet exchange points, domain name system service providers, and top level domain name registries).

Regulation (EC) no. 460/2004 repealed by Regulation (EU) no. 526/2013[20] established the European Network and Information Security Agency (ENISA), the core organisation on the EU level in the area of implementing measures in CS/IS, cooperation among the countries and reacting on concrete issues in this field. ENISA organises regular crisis exercises with hundreds of participants to train experts, fosters cooperation amongst them and provides guidance on best practices, provides expert trainings on crisis management, crisis planning or exercise development, conducts studies and organises international conferences on the topic of cyber crisis cooperation. ENISA Cyber Security Training material was introduced in 2008, and has been complemented ever since; it contains essential guidelines for success in the CSIRT community and in the field of operational security. An excellent example to the above said is ENISA's**Strategy for incident response and cyber crisis cooperation,** publishedinAugust2016[21] - a high-level summary of the basics of incident response, focusing on the work of Computer Security Incident Response Teams (CSIRTs) as key players in it.

Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, the 'European Programme for Critical Infrastructure Protection (EPCIP)[22] sets out the overall 'umbrella' approach to the protection of

[17]Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions European Strategy For A Better Internet For Children, Com(2012) 196 Final
[18]Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[19]However, EU Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify the so-called 'operators of essential services', envisaged by it.
[20]Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance, Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526
[21] Available at: https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[22]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, Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

critical infrastructures in the EU. The directive recalls for the identification of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include trans-boundary, cross-sector effects resulting from interdependencies between interconnected infrastructures. Such critical infrastructure should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures should be done under a common minimum approach.

Directive 2013/40/EU of the European Parliament and of the Council "On attacks against information systems"[23] introduced new rules harmonising criminalisation and penalties for a number of offences directed against information systems, and in doing so, complemented the Budapest convention. These rules call for EU countries to use the same contact points used by the Council of Europe and the G8 to react rapidly to threats involving advanced technology. The main types of criminal offences covered by this directive are attacks against information systems, ranging from denial of service attacks designed to bring down a server, to the interception of data and botnet attacks. Therefore, this directive focuses mainly on ensuring that the same offences are criminalised in all Member States and giving law enforcement authorities the means to act and to cooperate with one another. To this end, EU countries must have an operational national point of contact and use the existing network of 24/7 contact points.

3.3 International Soft Law

The activities of the United Nations (UN) regarding cybersecurity can be defined as highly fragmented, as the topic is addressed in many of its different intergovernmental bodies and organisational platforms/agencies[24]. Addressing this deficiency, the UN's Chief Executives Board for Coordination[25] has set up the UN Group on Cybercrime and Cyber Security in 2013[26], which tasked the International Telecommunication Union (ITU) and United Nations Office on Drugs and Crime (UNODC) to come up with a framework document for future inter-agency cooperation. In a follow up, the UN-wide Framework on Cybersecurity and Cybercrime was developed in 2013, and building on that document, the UN System Internal Coordination Plan on Cybersecurity and Cybercrime in 2014[27]. This document was designed as a guide to improve internal coordination activities of the UN system organisations on related matters. It is, however, the work of the **UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security** that has been under the spotlight with its work recently: the GGE Report in 2015[28] contains voluntary norms for state behaviour in cyberspace, including that nations should not intentionally damage each other's critical infrastructure or CERT with cyber-attacks, and should assist other nations in investigating cyber-attacks and cybercrime in their territories. Even though only about 20 countries have their representatives in the GGE, the work of the group since

[23] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040

[24] Tim Maurer, "Cyber Norm Emergence at the United Nations– An Analysis of the UN's Activities Regarding Cyber-security", Belfer Centre for Science and International Affairs, Harvard Kennedy School, 2011, available at: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

[25] The UN System Chief Executives Board for Coordination (CEB) is the longest-standing and highest-level coordination forum of the United Nations system. It meets biannually and is chaired by the UN Secretary-General. More information is available at: http://www.unsceb.org/content/about

[26] Action on Cybercrime and Cyber Security is available at: http://www.unsceb.org/content/action-cybercrime-and-cyber-security

[27] Available at: https://indico.cern.ch/event/391459/sessions/78824/attachments/1155155/1660100/ITU_CERN_9-09-2015.pdf

[28] Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

its first report in 2010 till today sets it as the key international mechanism for discussing - and eventually agreeing on - norms and confidence building measures in cyberspace, which countries should seriously take into consideration. It is worth noting that Serbia has its representative in this high-level UN-led group.

The focus of the work of the OSCE from its very inception has been to relax interstate relations. The rapid development of ICT has added a new, complex dimension to these relations, since despite all efforts, "cyberspace [still] constitutes an area with much room for speculation, doubt and ambiguity. The problem of attribution adds to the complexity, and increases the potential for tensions between the States".[29] The historical role of this organisation during the Cold War era as the political guardian of co-operative security has ultimately led to the creation and usage of specific mechanisms and documents, most important certainly being the Confidence Building Measures (CBMs). These measures are generally designed to help improve relations between states, achieve a peaceful settlement of a conflict or to prevent the outbreak of military confrontation. "Efforts to build confidence are important because they can prevent misunderstandings and stop an attack potentially escalating worldwide. They are like pressure valves, allowing a safe release of tensions".[30] Two decisions of the Permanent Council on CBMs are the most notable examples of the OSCE's involvement in cyber space, and are considered to be a breakthrough in this area[31]. **Decision no. 1106 with the initial set of OSCE CBMs[32]**, from 3 December 2013, aims to reduce the risks of conflict stemming from the use of information and communication technologies. These voluntary measures include: exchanging information on cyber threats; the security and use of ICT; national organisation, strategies, and terminology; holding consultations in order to reduce risks of misperception and of the possible emergence of tension; sharing information on measures taken to ensure an open and secure internet; exchange of points of contact; and the use of the OSCE as a platform for dialogue. **The second set of CBMs inDecision no. 1202[33],** from 10 March 2016 aims to expand a ground-breaking list of OSCE confidence-building measures, especially towards public-private partnerships (PPP).

As for the OECD, in July 2002 **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security[34]** was issued. The guideline suggests the need for a greater awareness and understanding of security issues and the need to develop a "culture of security". Furthermore,the **OECD Council Recommendation on the Protection of Critical Information Infrastructures[35]** provides a high level policy framework for the development of a national policy and international co-operation for critical information infrastructure protection (CIIP). The Recommendation reflects a shared understanding of the concept of Critical Information Infrastructures (CII) and of how national CII are identified across countries. The guidelines suggest the following when implementing national policies for the protection of the critical information infrastructure and cybersecurity programmes:

- A national strategy
- Legal foundations
- Incident response capability

[29] Available at: http://www.osce.org/secretariat/cyber-security
[30] Available at: http://www.osce.org/secretariat/106324
[31] *ibid.*
[32] Available at: http://www.osce.org/pc/109168?download=true
[33] Available at: http://www.osce.org/pc/227281?download=true
[34] Available at: https://www.oecd.org/sti/ieconomy/15582260.pdf
[35] Available at: https://www.oecd.org/sti/40825404.pdf

- Industry-government partnerships
- A culture of security
- Information sharing mechanisms
- Risk management approach

The North Atlantic Treaty Organisation (NATO), being a collective defence organisation, focuses its cybersecurity-related efforts on cyber defence. NATO has followed the rapid changes in the threat landscape instigated by the increased dependence on technology and the Internet and has therefore firmly embedded cyber defence in its strategic and institutional framework. Changes even happened in the doctrinaire framework of the organisation, as the 28 member states agreed in 2016 to declare cyberspace as its operational domain, in addition to air, land and sea[36]. The current **NATO cyber defence policy**[37], adopted in 2014 at the Alliance's Wales Summit, contains, among others, procedures for assisting the Member States (MS), defining ways to take awareness, education, training and exercise activities forward and emphasising the need for progress in further cooperation initiatives – with partner countries, other international organisations as well as with the industry. Although NATO's top priority in cyber defence is the protection of communication and information systems (CIS)[38] owned and operated by the organisation, it also relies on a reliable and secure national infrastructure of its member states.

The NATO-accredited Cooperative Cyber Defence Centre of Excellence (CCD COE), launched the Tallinn Manual Process in 2009 "as a leading effort in international cyber law research and education" which consisted of research and practitioner-oriented training programmes, with **Tallinn Manual on the International Law Applicable to Cyber Warfare**[39] as the key international document providing proposals related to the application of the international law to cyberspace. CCD COE has also developed a comprehensive **National Cyber Security Framework Manual**[40], which provides detailed background information and in-depth theoretical frameworks to help understand the various facets of National Cyber Security, according to different levels of public policy formulation. The four levels of government — political, strategic, operational and tactical/technical — each have their own perspectives on National Cyber Security, and each is addressed in individual sections within the Manual. Additionally, the Manual gives examples of relevant institutions in National Cyber Security, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions.

The listed mechanisms confirm that the direction in which the cybersecurity environment should be built in countries of theWestern Balkans is clearly set by key international and regional mechanisms as well as voluntary measures. Transposing agreements and directives into national laws is an important, albeit first step - equally important is the implementation, which requires political will and then strategic approach to cybersecurity and capacities for implementing the action plans, including through cooperation with other stakeholders, especiallythrough public-private partnerships.

[36] Statement by NATO Secretary General following the North Atlantic Council meeting at the level of NATO Defence Minister, available at: http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en
[37] Available at: http://www.nato.int/cps/en/natohq/topics_78170.htm
[38] *ibid.*
[39] Available at:https://ccdcoe.org/tallinn-manual.html
[40] Available at: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

4 State of play in the Western Balkans

There is no research available that specifically tackles the developments in the Western Balkans in the area of cybersecurity. Nevertheless, several related global reports also reflect the situation in some or most countries of the region, such as the ITU's "2015 Global Cybersecurity Index and Cyberwellness profile"[41] and the BSA's "EU Cybersecurity Maturity Dashboard 2015"[42]. Certain reports are available that focus only on particular aspects of cybersecurity, such as the ITUassessment of the needs and capabilities to create national CIRTs under its IMPACT programme[43] and the OECD "Competitiveness in South East Europe: A Policy Outlook" of 2016[44]briefly indicating the status of cybercrime legislation and cybersecurity policy partnerships. The country reports of the European Commission on the state of play of each of the candidate countries from the Western Balkans cover the areas of information society and media as well as security, showcasing basic information related to cybersecurity. Due to its status, Kosovo* does not feature in many of the reports, yet a particularly relevant source of information for assessing the developments in cybersecurity is the research paper entitled "Cybersecurity Capacity Assessment of the Republic of Kosovo"[45], conducted in 2015 by the Oxford University's Global Cyber Security Capacity Centre with the support of the World Bank[46], It is based on the Global Cyber Security Capacity Centre's Cyber Security Capability Maturity Model methodology used on the Kosovo* case for the first time in the Western Balkans.

Building upon the findings of these reports as well as on additional research work, brief country profiles are presented focusing primarily on the level of maturity of the legal and policy framework (such as the umbrella law, national strategy with action plan, and compliance with related international frameworks) and the establishment of the operational framework (such as the competent national authorities, cyber-incident response teams - CERTs, cybercrime and defence units and related capacities), but also taking into consideration possible comprehensive approaches to public-private partnerships and multistakeholder cooperation formats as well as strategic education initiatives. The summary offering a "zoom-out" perspective on the region is provided afterwards.

4.1 Albania

Albania's road towards safer and more resilient cyberspace has begun with the National Cross-cutting Strategy on Information Security (2008-2013). The document briefly mentioned cybersecurity as one of the areas to be considered as a priority. The Strategy also envisaged the creation of the National Agency for Cyber Security (ALCIRT)[47] as the national institution for response to cyber-incidents. ALCIRT, placed under the Prime Minister's authority, was created in 2011 with the support of the USAID's Albanian Cyber Security Program, involving training workshops provided

[41] Available at: http://www.itu.int/pub/D-STR-SECU-2015
[42] Available at: http://cybersecurity.bsa.org/
[43] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/assessmentEur.pdf
[44] Available at http://www.oecd.org/publications/competitiveness-in-south-east-europe-9789264250529-en.htm
[45] Available at:https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Kosovo_June_2015.pdf
[46] "The World Bank Supports Kosovo's Efforts in Strengthening Cyber Security", available at: http://www.worldbank.org/en/news/press-release/2015/06/25/world-bank-supports-kosovo-efforts-in-strengthening-cyber-security
[47] R.Bofati and J.Josifi: "Towards a more resilient cyberspace: the case of Albania", Information & Security: An International Journal, vol. 32, 2015, available at: https://procon.bg/system/files/3310_albania.pdf

to the government and non-government sector by the Carnegie Mellon University's Software Engineering Institute (SEI) towards building skills to resist operational threats and develop processes for managing cybersecurity incidents[48].

ALCIRT is also in charge of participating in preparing the national cybersecurity strategy, drafting relevant legislation, cooperating with all relevant institutions, international organisations, CSOs and the private sector and organising awareness campaigns, trainings and education materials on ICT). Nevertheless, with only six employees (the director and five experts), it has very limited human and infrastructure capacities and was not able to perform well both on responding to cyber-incidents and on wider activities such as education and initiating sustainable public-private partnership networks.

In 2014, ALCIRT took the initiative and led the interagency group for drafting the National Policy Paper on Cybersecurity for the period 2015-2017. The document was recently adopted and is aimed to assess the current situation and trends in relation to cybersecurity in the country. However, a national cybersecurity strategy still does not exist, although Working Group for the drafting of the strategy is created.Also, the first draft of the CS law exists and is currently under scrutiny by the main stakeholders in this area. It should be adopted by the end of 2016.

As opposed to other countries of the region, cybersecurity and cyber-defence is high on the agenda of Albania's defence-related institutions. In this regard, Albania's National Security Strategy (2014-2020) classifies cyber-attacks as a type one (highest importance) risk[49]. As a member of NATO, Albania signed the MoU with the NATO Cyber Incident Response Centre (NCIRC) on enhancing cyber defence in 2013 and is currently negotiating the signing of the new version of this MoU. This version is based on the cyber defence document "NATO Enhanced Cyber Defence Policy", endorsed by all NATO countries at the Wells summit in 2014[50]. Moreover, Albania took part in the annual Cyber Coalition exercise, NATO's largest cyber exercise, as an observer country twice, and will become an active participant as of November 2016. Albania also actively participates in NATO's cybersecurity related projects[51]. At the same time, Albania is formally implementing the initial set of OSCE "Confidence Building Measures" for cyberspace as of 2014, and has agreed in principle to further continue the process at hand with the approval of the second set of CBMs.

4.2 Bosnia and Herzegovina

Bosnia and Herzegovina (BIH) has not adequately progressed in the cybersecurity field, nor has it harmonized its legislation accordingly and still lacks a comprehensive overall strategic approach to address the issue of cybercrime and cybersecurity threats[52]. Namely, just as it is the case with the security management structure in Bosnia and Herzegovina, the legislation in the country reflects the complex and decentralised organisation of the country. The existing legislation on the state level that may be related to cybersecurity only scarcely and partially addresses relevant issues, and has

[48] Available at: https://www.usaid.gov/albania/press-releases/usaid-completes-project-support-albania%E2%80%99s-new-cyber-incident

[49] Available at: http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf (in Albanian)

[50] Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[51] Albania is the board member in NATO-s smart defence project "Multinational Cyber Defence Education and Training" (MN CD E&T), available at: http://ncia.nato.int/Documents/Agency%20publications/Communications%20and%20Information%20Partnerships%20and%20Multinational%20Projects.pdf

[52] European Commission, "Bosnia and Herzegovina 2015 Report", page 63, available at: http://ec.europa.eu/enlargement/pdf/key_documents/2015/20151110_report_bosnia_and_herzegovina.pdf

not fully implemented the provisions of the international framework it adheres to, such as the Convention on Cybercrime[53].

BIH does not have a state-level law on information security. Instead, its entity, RepublikaSrpska, has adopted the Law on Information Security. Also, the only document on the state level that directly tackles cybersecurity issues is the Strategy for Establishment of a CERT in Bosnia and Herzegovina[54]. However, although this Strategy was adopted in 2011, and the Working Group (WG) envisaged the BIH-CERT to be created[55], it still does not exist and the Action Plan drafted by the WG is still pending adoption due to political reasons. On the other hand, the Department for Information Security within the Agency for Information Society of the RepublikaSrpska became operational in June 2015[56]. This unit is tasked to coordinate prevention of and protection from computer security incidents and to supervise implementation of standards and measures of information security, but only in RepublikaSrpska. It cooperates closely with relevant departments of the Ministry of Interior of RepublikaSrpska, especially its High-Tech Crime Prevention Unit.

As for the possibilities in education, BIH hosts the South-East Europe Cyber Security Centre (SEECSC) – a research and development unit at the American University in Bosnia and Herzegovina[57]. The university offers cybersecurity education (both on a professional and academic level – through MA and PhD courses) and cooperates with security, intelligence and defence institutions in BIH.

4.3 Croatia

As the only EU member state in the region, Croatia was obliged to complete the institutional and legal framework in the cybersecurity area during its accession process. For this reason, it has fully enacted all the necessary laws and regulations and made them compatible with the EU regulation. To this end, Croatia adopted its Law on Information Security in 2007, which stipulated the creation of a national CERT (n-CERT), the so-called CARNet[58]. Its main task is the processing of incidents on the Internet, i.e. preservation of information security in Croatia. In addition, there is also a government CERT called ZSIS-CERT, situated in the Information Systems Security Bureau (ISBB). The ISBB is the central state authority responsible for technical areas of information security of the Republic of Croatia state bodies, which includes: creating standards of information security, security accreditation of information security, managing crypto material used in the exchange of classified information, and coordination of prevention and response to computer threats to information system security. Other legal documents completing the Croatian CS framework are the Security and Intelligence Systems Act of the Republic of Croatia (2006)[59], the Data Secrecy Act (2007)[60],

[53] S. Barakovic and J. BarakovicHusic: "'We have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina", Information & Security: An International Journal, vol. 32, 2015, https://procon.bg/system/files/3205_bih_barakovic.pdf

[54] Unlike the EU practice which looks at adopting the generic law on information security through which the operational bodies are also defined, here the strategic level document is used to establish the operational body. The document is available at: www.msb.gov.ba/docs/Strategija_za_CERT.doc.

[55] BIH-CERT is stipulated to be an expert body of an advisory and coordinating nature

[56] *ibid. 51*

[57] More on SEECSC on page 41

[58] Available at: http://www.cert.hr/en/start

[59] Available at: https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Security%20and%20Intelligence%20System%20Act.pdf

[60] Available at: https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Data%20Secrecy%20Act.pdf

Regulation on Information Security Measures (2007)[61] and Act on Critical Infrastructures (2013)[62]. All these show a well-rounded legal and operational environment.

The National Cyber Security Strategy of the Republic of Croatia and the Action Plan for its implementation were adopted in October 2015[63]. This overarching strategy is the most comprehensive and systematic strategic document related to cybersecurity in the Western Balkans. The strategy aims to "…achieve a balanced and coordinated response of various institutions representing all the sectors of society to the security threats in modern-day cyberspace. The Strategy recognises the values that need to be protected, the competent institutions and measures for systematic implementation of such protection"[64]. It clearly stipulates the need for the creation of strategic documents related to cyber-defence and cybercrime respectively.

On an institutional level, the Strategy assumes the creation of the National Cyber Security Council, which will have large competencies in monitoring and coordination of the implementation of the Strategy, its possible changes, and in proposing the organisation of national exercises. However, its work is not constrained to monitoring the implementation of the Strategy – it has the authority to address issues essential for cybersecurity management and, among other things, to issue periodic assessments of the state of security and define the cyber crisis action plan. On the technical level, the Council will be supported by the Operational and Technical Cyber Security Coordination Group, and more importantly, it is tasked to submit reports directly to the Government.

Finally, although the Strategy stipulates the need for strong public-private partnerships, there is no evidence of such for the time being in Croatia. At the same time, some forms of professional education and capacity building are conducted by the ISBB, the national CERT and the university Center for Information Security.

4.4 Kosovo*

Kosovo* does not have a stand-alone law on cybersecurity. Nevertheless, legal provisions on ICT and the protection of personal data exist respectively within the Law on Electronic Communications and the Substantive Law on (Prevention and Fight of) Cyber Crime[65].

In January 2016 the Government of Kosovo* adopted the "National Cyber Security Strategy and Action Plan 2016-2019"[66]. The Strategy envisages that the Law on Identification and Protection of Critical Infrastructure will be drafted in the course of 2016, with the CIIP being an important part of this law. Also, the Strategy stipulates the need to review the Law on Preventing and Combating Cybercrime.

The lead ministry for drafting the Strategy was the Ministry of Interior Affairs (MIA) which formed the Working Group (WG) in 2015. Interestingly enough, the WG included a variety of actors – all state institutions, professional associations, the private sector, civil society and international partners. The Strategy envisages some thought-provoking institutional solutions to achieving its

[61] Available at: https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Regulation%20on%20information%20security%20measures.pdf
[62] Available at: http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama
[63] Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/croatian-cyber-security-strategy/view
[64] *ibid. 60*
[65] Law no. 03/L-166, Law on Prevention and Fight of the Cyber Crime, available at: http://www.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf
[66] National Cyber Security Strategy and Action Plan 2016-2019, available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-national-cyber-security-strategy-and-action-plan-2016-2019

main objectives[67], such as appointing the National Cyber Security Coordinator, "…mandated to coordinate, guide, monitor and report on the implementation of policies, activities and actions in connection with the National Cyber Security Strategy"[68]. The Strategy envisages that the Minister of Internal Affairs (or the person authorised by him) shall be appointed as Coordinator, thus giving political leverage and significance to implementing the Strategy. This important political message is accompanied with the creation of the so-called Secretariat of the Strategy, the body in charge of monitoring and coordinating the activities of the Strategy. Finally, in an effort to foster coordination of the competent and relevant government authorities and representatives of the private sector, the Strategy envisages the creation of the National Cyber Security Council. The creation of the Council is a unique solution in the Western Balkans for enhancing and even enforcing cooperation of different institutions within the government, but also for creating meaningful and potentially powerful public-private partnership.

With heavy assistance of the EU-funded project ENCYSEC, KOS-CERT[69] has recently started working as n-CERT ("National Computer Security Unit"). It is still a work in progress, but the vision of creating a small, highly-skilled team responsible for incident reporting and handling, as well as coordinating awareness-raising activities on the national level is present. KOS-CERT is a functional unit within the Regulatory Authority for Electronic and Postal Communication.

Although the existence of the Strategy and its ambitious goals show that cybersecurity has been recognised as a priority across the government, a number of other factors show that Kosovo* is still in the initial phase of developing cybersecurity capabilities. Cybersecurity education is scarce and exists in fragments only at the University of Pristina; training programmes exist only in an ad-hoc manner; cybersecurity awareness is limited and basic and needs to be fostered among different parts of the population in different manners. However, a number of these deficiencies have been recognised in the Strategy and addressed in the Action Plan.

It should be noted that the whole process is still to a large extent donor-driven. This is mostly visible in the Action Plan, which has a column for each designated activity stating the supporting institution for the activity – a large number of the activities are to be supported by 'international partners', namely the US "International Criminal Investigative Training Assistance Program" (ICITAP), the EU's "Enhancing Cyber Security" (ENCYSEC) pilot programme, the UNDP and the OSCE. It is unclear, though, whether the international organisations (apart from ENCYSEC project) have already committed themselves to assist heavily in developing a cybersecurity framework or this is just a wish-list of the WG which drafted the Strategy. Still, having in mind that the representatives of the international organisations were part of the WG, the first option seems to be more probable.

4.5 Montenegro

Montenegro has advanced fast in the cybersecurity area since 2010 when the umbrella piece of legislation – Law on Information Security - was adopted, along with the Regulation on Information Security Measures. A national Cyber Security Strategy for Montenegro for the period 2013-2017 was adopted in October 2013. Action plan for Strategy implementation for the period 2013-2015 is part

[67] The objectives are: CIIP, institutional development and capacity building, building public and private partnerships, incident response and international cooperation.
[68] National Cyber Security Strategy and Action Plan 2016-2019, page 15.
[69] KOS-CERT description following IETF RFC 2350 for CIRT, available at: http://kos-cert.org/assets/cms/uploads/files/KOS-CERT%20RFC2350.pdf

of the Strategy as an Annex, though there was no Action plan for the period 2015-2017 at the time of publishing this report.

In terms of an institutional framework, the first task envisaged by the Action plan was the establishment of the National council for cybersecurity/information security. This has not happened to date, although it was again in line with the amendments of the Law on Information Security, adopted in January 2015. Once operational, the Council is supposed to be the key institution related to cybersecurity issues. The Council will also be in charge of creating procedures for the regular exchange of information between state authorities and key institutions from the private sector, i.e. internet providers, agents for .me domain, banking sector, electric power companies and companies that host e-services in Montenegro[70].

The national CIRT of Montenegro became operational in 2012, with the assistance of the ITU-IMPACT programme. The n-CIRT is positioned in the Ministry of Information Society and Telecommunications and performs regular CIRT duties. The national CIRT is also very active in promoting the culture of being safe in cyberspace. In 2015, it developed the document titled "Guidelines for Security and Protection of Information in Cyberspace". In cooperation with the ITU, CIRT.me organised a cyber drill in September 2015 for CIRT/CERTs from Europe. The drill was attended by more than 50 participants from Montenegro and other countries. In addition, CIRT.me actively participates in the overarching TEMPUS project related to cybersecurity education in Montenegro.

In October 2014 the Government of Montenegro adopted the Methodology of identifying Critical Information Infrastructure (CII) and the Action plan for its implementation. This document was prepared and published despite the lack of a Law on critical infrastructure of Montenegro, and due to the importance of making additional progress in this area. This is the only national document related to CII in the Western Balkans. Moreover, in 2015, the Ministry for Information Society and Telecommunications developed the methodology for assessing the cybersecurity capacity maturity model. This methodology was drafted with the financial assistance of the World Bank and in cooperation with the Oxford University Global Cybersecurity Centre's existing Cybersecurity Capacity Maturity Model.

Montenegro has an official university master-level program on cybersecurity policy, developed and delivered by the DonjaGorica University in Podgorica, which gives a unique mix of technical and policy-based knowledge on a variety of cybersecurity issues. The DonjaGorica University is also a partner in the above mentioned EU-funded TEMPUS project.

4.6 Republic of Macedonia

Macedonia does not have an overarching law dealing exclusively with cybersecurity. Instead, a number of legal documents touch upon some cybersecurity related issues – the Law on Personal Data, the Law on Electronic Commerce, the Law on Electronic communications, the Law on Interception of Communications, the Law on free Access to public Information, the Law on Data in an Electronic Form and Electronic Signature. In addition, the amendments to the Law on Criminal Procedure adopted in 2013 specifically tackle cybercrime and crimes committed with the use of computers, as well as the collection of digital evidence by the law enforcement authorities.

[70] Action no.6 at the National Action Plan accompanying the National Cybersecurity Strategy of Montenegro, available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Montenegro_2013_Cyber%20Security%20Strategy%20for%20Montenegro.pdf

Although some international organisations facilitated discussions during the preparation of the National Cybersecurity Strategy (for example, the UNDP commissioned an Assessment Study for the Requirements for Preparation of a National Cyber Security Strategy), the national Strategy is still in the drafting process[71].

The national academic and research network MARnet, created in 2010, took over the capabilities and duties of the academic CERT, which was previously situated in the Ss. Cyril and Methodius University in Skopje. However, with an impetus acquired through implementation of the EU-funded cybersecurity pilot project under the EU ENCYSEC, a national MKD-CERT was formed in 2015 as part of the Agency for Electronic Communication (AEC), performing regular CERT functions.

In terms of institutional capacities to deal with cybercrime issues, the Cybercrime Unit located within the Department for Suppression of Organised and Serious Crime and the Forensic Department of the Ministry of Interior merged into a single Cybercrime and Digital Forensic Department, thus forming a more efficient and effective investigative unit.

4.7 Serbia

Serbia's legal and institutional framework in the area of cybersecurity is based on the Law on Information Security, which was adopted at the beginning of 2016. Important bylaws (on protection measures, on the list of operators performing activities of public interest including critical infrastructure, on reporting incidents) are being drafted, though mainly within the government circles and without broader consultations. The Law stipulates that the operators of ICT systems of special importance (some of which will be listed as critical information infrastructure) have to adopt an act on ICT system security with dedicated protection measures, supervision of their ICT systems and persons responsible to perform these tasks. Furthermore, the Law envisaged the creation of the Body for the Coordination of Information Security, with the option of establishing expert working sub-groups that could include representatives of other public bodies, industry, the academic community and civil society[72].

The necessity to establish a proper cybersecurity related system has been recognised at the strategic level, in the Strategy for Development of Information Society in the Republic of Serbia until 2020 which puts information security as one of its six priority areas. As a follow-up, the Working Group for developing the national strategy on cybersecurity has been established in 2016 and has held its first sessions; the strategy is expected to be adopted by the in the first quarter of 2017. However, a critical information infrastructure has not been defined yet, and cybersecurity standards are not yet approved.

The Law mandated the creation of the n-CERT in the regulatory agency for electronic communications and postal services (RATEL). While formally established, it is in the development phase and currently lacks technical capabilities and resources; with proper capacity building, it is expected to become operational in 2017. At the same time, several other CERTs exist or are in formation: the academic CERT is part of the Academic Network (AMRES) and protects the network of education, scientific and research institutions; the Ministry of Interior has established its own CERT to protect sensitive citizens' databases and the system that operates the databases; the national Internet domain registry RNIDS is setting up the CERT for national domains .rs and .srb, while the

[71] EU FYROM Report 2015, available at: http://ec.europa.eu/enlargement/pdf/key_documents/2015/20151110_report_the_former_yugoslav_republic_of_macedonia.pdf(pp.20)

[72] Article 5, paragraph 2.Law on Information Society.*RS Official Gazette* no. 6/2016.

civil sector is working on establishing an independent CERT to help responding to attacks against the media. At the moment, however, there is no interaction among these.

Similar to other countries in the region, the legal mechanisms to fight cybercrime are in place. The Criminal Code provides norms on criminal offences in accordance with legal frameworks of theCoE and the EU. The Criminal Code does not regulate cyber terrorism as an offence, although cyber terrorism can be prosecuted on the basis of existing offences on terrorism and computer data. With regard to an institutional framework, a High-Tech Crime Unit within the special prosecutor's office has been established. Moreover three specialised units - for crime analysis; terrorism and extremism; and drug prevention, addiction and repression have been established within the MoI. All these units are in need of further staffing, and specialised training and adequate budgetary resources are needed. The level of inter-agency cooperation, information flow and exchange between law enforcement agencies needs to be further improved. However, internal cooperation between the police and the special prosecutor's office for cybercrime is improving.

There is no proper multidisciplinary cybersecurity education on the policy level. General awareness-raising about online safety, especially among the youth, is tackled through the campaign "Smart and Safe" driven by the Ministry of Trade, Tourism and Telecommunications, but its scope is limited.

4.8 Regional summary

According to the review, there is progress in formally establishing the legal and operational frameworks in most of the countries of the Western Balkans, except for BIH and Macedonia which are lagging behind. They are all making efforts to meet the criteria for EU membership, and are being assessed regularly through the EU country reports (previously known as progress reports) published on a yearly basis (usually in October each year)[73]. Western Balkan countries are signatories of all the related Council of Europe agreements, enabling the provisions for those to become part of the domestic legal systems. Since all the countries are on the EU track, there is a formal follow-up on implementing the EU requirements as well, both on a policy and on an operational level. Table 1 summarises the status of development of the key cybersecurity elements of the national environment in each of the countries of the Western Balkans.

	ALB	BIH	CRO	KOS	MKD	MNE	SRB
CS/IS Law	-/+	-	+	-	-	+	+
Cybercrime (in) Law	+	+	+	+	+	+	+
CS/IS Strategy	-/+	-/+	+	+	-	+	-/+
n-CERT	+	-/+	+	+	+	+	+
Substantial PPP	-/+	-	-	-/+	-	-/+	-
CB/Education	-	-/+	+	-	-	+	-

Table 1: Cybersecurity environment in the Western Balkans: "+" denotes that (at least) the basics are in place, "-/+" denotes that some early developments are on the way, while "-" denotes there are no significant developments identified.

[73] Country reports are only stating whether a country has a national cybersecurity strategy in place and the level of preparedness of a country to tackle cybercrime.

There are significant differences and important similarities in the development of cybersecurity policy across the Western Balkan region. In most countries, specific legislation on information security seems to be in place. It is remarkable however, that Montenegro had already passed such a law in 2010, whereas in Serbia for instance, it was not adopted until early 2016. Bosnia and Herzegovina on the other hand has not yet managed to develop any significant state-level legislation on cybersecurity.

More progress seems to have been achieved with cybersecurity strategies and comprehensive risk assessments. Again, Montenegro has led the trend, whereas Serbia has yet to finalise a strategy and Bosnia and Herzegovina has not even started working on one. Still, Western Balkan countries seem to be slow in implementing strategies. Whereas progress is seen in some countries in making law enforcement activities in the field of cybercrime more efficient, staff at the CERTs and in LEAs generally still lack resources and capacities.

Hardly any serious educational policies have been undertaken in any of the countries in the region. Very little to no outreach to the private sector has happened and no significant public-private partnership with private sector actors have been set up.

5 Activities and support instruments of international organisations in the Western Balkans

Cooperation in the cybersecurity area can be successfully achieved through existing international organisations, which allow for the transfer of experiences and development assistance for building expertise and resources. Despite the efforts (invested especially by the UN), there is no one international organisation (IO) handling all CS-related issues – rather, they are scattered across different IOs' agendas, depending on the area the organisations cover, such as cybercrime, network security and CERTs, or international peace and security. There are efforts to introduce innovative, multistakeholder forms of international cooperation – this is particularly visible when dealing with the issues pertaining to Internet governance (World Summit on the Information Society and the Internet Governance Forum) - aiming to take away the exclusivity of dealing with these complex issues from the states and give more leverage to other important actors in a world which is rapidly changing. The private sector involved in CS, as well as expert organisations and academia, play an increasingly important role in such an environment, especially in terms of policy shaping and capacity building.

Major international players offering assistance in CS in the Western Balkans are the European Union (EU), the North Atlantic Treaty Organisation (NATO), the Organisation for Security and Cooperation in Europe (OSCE), the Council of Europe (CoE), the United Nations Development Programme (UNDP) and the International Telecommunication Union (ITU)[74]. Even though they are tackling different perspectives, their assistance activities frequently overlap due to a number of reasons, which lead to non-rational budget spending and poor utilisation of resources.

The countries of the Western Balkans are all, apart from Kosovo* (due to its still disputable international status), well embedded in international forums. All countries are members of the OSCE, the CoE; they all aspire to become full-fledged members of the EU (with Croatia already being an EU country); they all, apart from Serbia, aspire to become members of the NATO Alliance, with Croatia and Albania already NATO MS, Montenegro currently finalising the accession process and other countries having intensive cooperation with the Alliance. On the other hand, since the beginning of the Yugoslav wars, various UN agencies are heavily present in the region, with the UNDP being the most notable example.

This chapter of the research will therefore examine the roles and activities of international organisations in the Western Balkans in the cybersecurity area, and assess the level and success of their involvement.

5.1 The European Union (EU) and the Council of Europe (CoE)

The EU has given a clear membership perspective to all Western Balkans countries, on condition of meeting the necessary requirements ("The future of the Western Balkans is within the European Union" was the main message of the EU-WB Thessaloniki Summit in 2003)[75]. The two issues in focus in the EU country reports - combating cybercrime and developing national cybersecurity strategy - are tackled through different projects funded by the EU and implemented by different organisations.

[74] As the focus has been placed on the efforts of these IOs, the other organisations which only occasionally tackle the CS issues and bilateral cooperation of the Western Balkan countries with other countries/major players in this area are not part of this research.

[75] Available at: http://europa.eu/rapid/press-release_PRES-03-163_en.htm

Within the scope of its **Instrument contributing to Stability and Peace (IcSP)**[76], the European Commission funded a pilot project "Enhancing Cybersecurity (ENCYSEC)"[77], with beneficiary countries being Macedonia, Kosovo* and Moldova. The overall objective of the project was "to increase the security and resilience of ICT networks in the partner countries by building and training local capacities to adequately prevent, respond to cyber-attacks and/or accidental failures".[78] Expected results that were to be achieved during the time-span of the project (January 2014 – January 2016) were: creation and/or development of national CERTs and 24/7 contact points; adoption of the National Cybersecurity Strategies and awareness raising; development of public-private partnerships and international cooperation. The project was implemented by a consortium of two French consultancies close to the French Government. The choice of the beneficiary countries is not publicly available, yet the IcPS eligibility criteria required involving countries from at least two regions (Eastern Europe and Western Balkans). However, it is a pity that only some Western Balkans countries were engaged in the project. Also, the final outcomes of the project are not available, although it is clear that not all the initially envisaged outcomes were reached (KOS-CERT and national strategy are a direct product of the ENCYSEC assistance, whilst the establishment of the MKD-CERT might have been only impacted by the project).

As for its efforts in mitigating cybercrime threats, the EU has paired in this endeavour with the Council of Europe (CoE). Apart from its global project which (in three phases) included around 110 countries, two long-term projects have been organised specifically for the Western Balkans countries, under the framework of the Instrument for **Pre-Accession (IPA)** – **CyberCrime@IPA**(2010-2013)[79] and **iPROCEEDS** (2016-2019)[80].

The CyberCrime@IPA project is titled "Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime" and its beneficiary countries were Albania, BIH, Croatia, Montenegro, Macedonia, Serbia, Turkey and Kosovo*. The objective of the project was to "…strengthen the capacities of criminal justice authorities of project areas to cooperate effectively against cybercrime based on the Budapest Convention on Cybercrime and other standards and tools"[81]. Overall, according to the final report of the project, the progress was made on all the recommendations, most notably in raising awareness, enhancing cooperation between the public and private sectors as well as increasing regional and international cooperation against cybercrime.[82]

iPROCEEDS is another joint project of the EU and the CoE implemented under the umbrella of the IPA II Multi-country action programme 2014. The beneficiaries are the same as in the CyberCrime@IPA project with the exception of Croatia (since it has in the meantime joined the EU). The project started on January 1, 2016 and following the completion of the inception phase, has had its launching conference in Ohrid, Macedonia on June 13-14, 2016. Its' main objective is strengthening the capacities of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.

---

[76] IcPS is an instrument for financing the EU's external actions, intended for conflict prevention, peace-building and crisis preparedness - including cybercrime and cyber-threats - in third/partner countries . More information is available at: http://ec.europa.eu/dgs/fpi/what-we-do/instrument_contributing_to_stability_and_peace_en.htm

[77] Available at: http://www.encysec.eu/web/

[78] *Ibid.*

[79] Available at: http://www.coe.int/en/web/cybercrime/cybercrime-ipa

[80] Available at: http://www.coe.int/en/web/cybercrime/iproceeds

[81] Available at: http://www.coe.int/en/web/cybercrime/cybercrime-ipa

[82] "Assessment report, Criminal justice capacities on cybercrime and electronic evidence in South-eastern Europe", Data Protection and Cybercrime Division, Council of Europe, Strasbourg; available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a0d

As of 2014, the collaborative projects of the EU and the CoE are being implemented by the CoE's Cybercrime Programme Office (C-PROC). C-PROC is situated in Bucharest, Romania and became operational in April 2014. It meets its purpose through capacity building projects, aiming at "…supporting countries worldwide in the strengthening of their criminal justice capacities to respond to the challenges posed by cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime".[83]

As seen above, the EU's IPA funds are being used for enhancing capacities in cybercrime issues in the Western Balkans, mostly focusing its efforts on police cooperation. Strategy papers dealing with the Multi-country IPA II priorities confirm this – cybercrime is mentioned, although in the negotiation chapters related to security issues it is only one of the problems to be addressed. On the other hand, neither cybersecurity nor information security are mentioned as strategic issues to be tackled. However, this does not close the window of opportunity to use these funds for dealing with CS/IS issues either on the national or on the regional level. Namely, the key areas the IPA funds are aimed for are enhancing competitiveness and growth in the region; the development of ICT sector is important to achieve these two goals, and CS/IS is of paramount importance - especially for e-commerce and protecting the financial market as well as small and medium enterprises (SME), but also for cybersecurity and IT start-up industry.

If they use IPA funds for these purposes, countries of the Western Balkans would do best to utilise the Regional Cooperation Council (RCC)[84] and the Regional School of Public Administration (ReSPA)[85], since those two institutions are recognised as focus of IPA II activities. Bearing this in mind, the RCC's SEE Strategy 2020 states that its goal is boosting the ICT industry through empowering SMEs, and a well-designed project proposal might include information security as an important prerequisite to achieve this goal. ReSPA, on the other hand, is perceived by the IPA II programme as the main capacity-building institution in the region, and might thus be used to include some CS/IS activities in this regard.

Horizon 2020, or the EU Framework Programme for Research and Innovation, is the biggest EU research and innovation programme with nearly 80 billion Euros in funding available over 7 years (2014-2020). It is the successor of FP7 and FP6 programmes which paved the way for creating the EU's blueprint for smart, sustainable and inclusive growth and jobs. Among a number of topics available for funding, cybersecurity is explicitly stated in the "Secure societies – Protecting freedom and security of Europe and its citizens" programme area.[86] The working programme for 2016/2017 lists different calls related to critical infrastructure protection; assurance and certification; cybersecurity for SMEs, local public administration and individuals; economics of cybersecurity; increasing digital security of health related data on a systemic level; EU cooperation and international dialogues in cybersecurity and privacy research and innovation; cryptography; addressing advanced cybersecurity threats and threat actors; privacy, data protection, digital identities. Although some of these topics are of importance for the WB countries, the entities eligible for applying need both thorough knowledge of the lengthy application process, but also already established pan-European networks (since many calls require a team of at least three partners, and at least one of them being from an EU country). Despite these hurdles, it is an

[83] "Worldwide Capacity Building", Council of Europe, available at: http://www.coe.int/en/web/cybercrime/capacity-building-programmes
[84] More on RCC can be found on page 37
[85] More on ReSPA can be found on page 43
[86] Available at: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

immense opportunity for different institutions dealing with cybersecurity in the Western Balkans that has to be worked on.

5.2 The North Atlantic Treaty Organisation (NATO)

NATO works with individual countries to help them develop mechanisms to ensure an appropriate level of cyber defence for national communication and information systems (CIS). As for the NATO Member States from the Western Balkans, to date, Albania has used this venue of opportunity, working on setting up the cyber defence institutional and strategic framework. Croatia recently expressed interest to become a member of the Tallinn-based, NATO-accredited**Cooperative Cyber Defence Centre of Excellence (CCDCoE)**[87], but apart from that initiative, it has apparently not been heavily engaged in cyber defence issues. Out of NATO partner states, Montenegro[88] is part of NATO's **Membership Action Plan (MAP)** programme[89]. Its' "Report on Implementation of the Fifth Annual National Programme of Montenegro in the period of intensified and focused discussions with NATO" contains an entire chapter on cybersecurity (chapter 4.2)[90], with four activities that are already part of the Action Plan for implementation of the National Cybersecurity Strategy. Serbia, while not aiming for the membership, runs an **Individual Partnership Action Plan (IPAP)** as an optimal framework of cooperation with NATO[91]. Its' first IPAP contains a section on emerging security challenges, among which is also cyber defence, yet it merely states that Serbia "wishes to enhance its capabilities for protecting critical communication and information systems against cyber-attacks" and that "government-level mechanisms and a coordination structure for cyber-defence need to be established"[92].

Apart from assisting individual member states and partner countries, NATO aims to enhance the level of preparedness for cyber-attacks through its unique Smart Defence initiative[93] which encourages Allies to cooperate in developing, acquiring and maintaining military capabilities to meet current security problems. Essentially, "NATO Smart Defence means pooling and sharing capabilities, setting priorities and coordinating efforts better"[94]. In the area of cyber defence, there are already three Smart Defence projects: **Multinational Cyber Defence Capability Development (MN CD2)**[95], **Malware Information Sharing Platform (MISP)**[96], and **Multinational Cyber Defence Education and Training (MNCDE&T)**[97]. As discussed earlier, Albania is the only country actively participating in one of these projects, namely MNCDE&T, where it is a Board member. However, these projects have huge potential for fostering cooperation and coordination among the Western Balkans countries in

[87] Ministry of Foreign Affairs of Estonia: "Kaljurand in Croatia: We must deal with security threats from both the east and south", available at: http://www.vm.ee/en/news/kaljurand-croatia-we-must-deal-security-threats-both-east-and-south
[88] Montenegro was officially invited to become the organisation's 29th member state on May 19, 2016. More information is available at: http://www.nato.int/cps/en/natohq/topics_49736.htm
[89] Available at: http://www.nato.int/cps/en/natolive/topics_37356.htm
[90] "Report on Implementation of the Fifth Annual National Programme of Montenegro in the period of intensified and focused discussions with NATO", available in Serbian only.
[91] Dijanalvancic, The Head of Department for NATO and Partnership for Peace at the Ministry of Foreign Affairs of the Republic of Serbia, in "NATO and Serbia agree first Individual Partnership Action Plan", available at: http://www.shape.nato.int/nato-and-serbia-agree-first-individual-partnership-action-plan
[92] "Individual Partnership Action Plan Republic of Serbia and NATO", available at: http://www.mfa.gov.rs/en/images/ipap/ipapeng.pdf
[93] Available at: http://www.nato.int/cps/en/natohq/topics_84268.htm
[94] Frosina Doninovska, "The concept of Smart Defence and sharing defence capabilities among states", available at: http://www.iapss.org/2014/09/24/the-concept-of-smart-defence-and-sharing-defence-capabilities-among-states/
[95] Available at: https://mncd2.ncia.nato.int/Pages/default.aspx
[96] Available at: http://www.misp-project.org/
[97] Available at: http://ncia.nato.int/Documents/Agency%20publications/Communications%20and%20Information%20Partnerships%20and%20Multinational%20Projects.pdf

the cyber defence area for several reasons: technically, they are open for both member states and partner countries (on condition of signing an MoU), meaning that all countries of the WB are eligible to participate on an equal footing; secondly, the underlying idea behind the Smart Defence initiative is to foster cooperation between countries with similar capabilities, or with common equipment requirements, and this certainly goes for all the Western Balkan countries; finally acting together in the scope of this programme may assist countries to develop capabilities which they could not afford individually, and to share considerable costs thereof.

Another policy tool of NATO which might be well used for cooperation of the Western Balkan countries in the cyber defence area is the **Science for Peace and Security Programme (SPS)**. The very basis of the programme is to promote security-related cooperation to address emerging security challenges. Its main aim is to connect scientists, experts and officials (government or civil society based) both from member states and partner countries to address these challenges[98]. One of the three pillars of this programme - next to science and security - is partnership, thus focusing its efforts on collaborative frameworks. Cybersecurity threats and, more specifically, cyber defence are some of the security areas this program focuses on. They are placed in the programme's first key priority – "Facilitate mutually beneficial cooperation on issues of common interest, including international efforts to meet emerging security challenges", and include the following sub-topics:

- Critical infrastructure protection, including sharing of best practices, capacity building and policies;
- Support in developing cyber defence capabilities, including new technologies and support to the construction of information technology infrastructure;
- Cyber defence situational awareness.[99]

Collaboration within the SPS programme is made possible through a variety of grant mechanisms and formats, thus enabling the beneficiaries to maximise the effect of the funding using the most appropriate format. Applicants have at their disposal multi-year projects (MYP) with significant funding, training courses meant for post-doc level scientists (Advanced Training Institute ATI) or for an expert audience (Advanced Training Courses - ATC), and workshops (Advanced Research Workshops - ARW) intended to foster advanced level discussions on some of the SPS key priority areas. The variety of mechanisms on the 'menu', as well as the requirement to include at least one NATO and one Partner country as co-organisers fits perfectly the needs of the WB countries. NATO members (Croatia and Albania) could therefore connect with their peers from the other WB countries in an effort to utilise these opportunities.

The Western Balkan countries have up to now used the SPS programme for developing their scientific and policy capabilities in different fields, with cyber defence being only one of them. However, the feeling is that this resource was scarcely used and rarely to never as the result of a joint effort coming from the region. Statistics prove this statement – there were only six events organised within the scope of the programme and related to cybersecurity where the WB countries were partners – five ATCs and one ARW. Macedonia was the most agile WB country in utilising the opportunities this programme gives and organised as much as three events which saw the participation of experts from throughout the region – the first ATC was organised in October 2013 in Ohrid (Macedonia) and titled "NATO Regional Summer School on Cyber Defence (NATO RSSCD)" in

[98] "The NATO Science for Peace and Security Programme", available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151218_151218-sps-eng.PDF
[99] *ibid.*

cooperation with Slovenia[100]; ATC "Terrorist use of cyberspace" was organised in December 2014 in Ohrid (Macedonia) with Turkey as a NATO country co-organiser[101], whilst ARW was organised in March 2015 in Skopje (Macedonia) with a Bulgarian organisation as a co-organiser and titled "Encouraging Cyber Defence Awareness in the Western Balkans"[102]. The other three events are part of a specialised series of ATCs – Turkey has developed a "Hands-on training for system/network administrators" on the resilience of the national IT-structures and conducted it in Montenegro in 2013[103], whilst Estonia cooperated with Montenegro (February 2016)[104] and with Bosnia and Herzegovina (May 2016)[105] in delivering specialised cyber defence trainings for civil servants of the two countries respectively.

In conclusion, NATO offers a variety of possibilities for cooperation via individual partnerships with its MSs and Partner countries, but also through its different initiatives. WB countries have used these opportunities to some extent, but usually scarcely or individually, without motion or impetus to pair up and utilise available funds in a more appropriate manner. Eventually, the beneficiaries of these programs are not only state institutions, and it seems that non-state actors in the region are not fully aware of the available options for cooperation and collaboration in the cybersecurity area.

5.3 The United Nations Development Programme (UNDP)

The ITU and UNODC suggested in 2013 that the UNDP becomes "the lead agency in ensuring that cybersecurity programmatic assistance is provided on an 'on demand' basis to developing nations".[106] The UNDP therefore, as of 2014, offers cybersecurity services to countries – CS training workshops, CS risk assessment/mitigation, capacity building in cyber-incident response, resiliency, developing or reviewing cybersecurity policies and standards, and ISO 27001 certification.[107][108] Since UNDP is the main development agency in the region, with firmly embedded country offices, it presents an immense opportunity for fostering the development of national cybersecurity frameworks, but also in enhancing regional cooperation on this level.[109]

However, up to now, this new role of the UNDP has not been utilised in the Western Balkans, although there were/are opportunities to add cybersecurity to the UNDP´s portfolio in this sub-region. Namely, the UNDP in Albania has been supporting the Government of Albania to improve ICT infrastructure and e-services for more than a decade. The UNDP office in Tirana has used a variety of tools to assist the Albanian government in achieving its 'Digital Albania' goal: policy advice for managing the information society agenda of the government; advisory services in specific directions of the ICT agenda; assisting the government in deploying e-services. The UNDP in Serbia has also as

[100] Available at: http://www.pf.uni-lj.si/media/nato_poster_ohrid.pdf
[101] Available at: http://sites.miis.edu/cyber/2014/12/20/executive-education-december-2014/
[102] Available at: http://www.atlantic-club.org/index.php?advanced-research-workshop-8220encouraging-cyber-defence-awareness-in-the-balkans8221
[103] Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20141211_SPS_Annual_Report_2013.pdf
[104] Available at: http://www.nato.int/science/country-fliers/Montenegro.pdf
[105] Available at: http://www.nato.int/science/country-fliers/BiH.pdf
[106] Available at: http://www.csoconfab.com/wp-content/uploads/2016/03/CSO50_2016_Paul-Raines_Providing-Effective-Cybersecurity.pdf
[107] *ibid.*
[108] In its first year of involvement in cybersecurity on the UN-wide level, the UNDP paired with the EU ENCYSEC project and the network of CERTS - FIRST - in the organisation of the Istanbul FIRST Technical Colloquium and & TRANSITS training. More information is available at: https://www.first.org/events/colloquia/istanbul2015
[109] The UNDP has experience in implementing regional security sector-related activities/projects. See for example http://www.seesac.org/index.php

of recently started its Open Data Initiative in Serbia, in cooperation with the World Bank and in collaboration with the Serbian Ministry of Public Administration and Local Self-Government.[110]

Still, the only purely cybersecurity initiative of the UNDP in the Western Balkans came from the UNDP office in the Republic of Macedonia. Having in mind that developing national capacities to respond and effectively manage the EU accession agenda represents the overarching objective of the UNDP's country programme, upon request of the government's Secretariat for European Affairs, the UNDP assisted the national institutions in the reforms within the chapters related to security, whereby the necessity for designing and adopting a National Cyber Security Strategy was especially underlined. The UNDP offered to prepare an Assessment Study for the Requirements for Preparation of a National Cyber security Strategy. However, no data is available on what actually happened with the assessment study or the work of the working group.

5.4 The Organisation for Security and Cooperation in Europe (OSCE)

The OSCE is involved with cybersecurity in relation to international peace and stability, countering terrorism and cybercrime. Of particular importance for the cooperation in the Western Balkans is the second set of the OSCE CBMs, adopted in 2016, since it emphasises the need for regional and subregional collaboration; it also calls Participating States to "promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs"; and it particularly encourages regional and subregional collaboration "…between legally-authorised authorities responsible for securing critical infrastructures…"[111].

Apart from CBMs and direct inter-state relations, there are other mechanisms which the OSCE uses to promote responsible behaviour in cyberspace. It is worth mentioning that the structure of the organisation also enables a participating state which holds the Chairmanship to put an emphasis on certain topics. For the first time after the end of the Cold War, in 2015, a participating state from the Western Balkans, namely Serbia held the chairmanship, in coordination with Switzerland as the 2014 chair; their Joint Workplan, presented in 2013 listed cybersecurity and further development of OSCE contributions in this field as one of the priorities of this experimental joint effort.[112] Following that, both countries have focused on emerging threats from cybersecurity in their Chairmanship priorities[113], and organised events accordingly. In 2014, under the Swiss chairmanship, the OSCE meeting was organised in Vienna to support the activities of the Informal Working Group that developed the CBMs.[114] Serbia, on the other hand, organised an OSCE-wide event in Belgrade in October 2015 aiming to shed new light on effective strategies to cyber/ICT threats, mostly

[110] "Open Data: Open Opportunities", UNDP in Serbia, available at: http://www.rs.undp.org/content/serbia/en/home/ourperspective/ourperspectivearticles/open-data--open-opportunities.html

[111] OSCE Permanent Council, "Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", available at: http://www.osce.org/pc/227281?download=true

[112] "Joint Workplan of Switzerland and Serbia", available at: http://www.mfa.gov.rs/en/images/stories/slike/Joint-work-plan.pdf

[113] Available at: http://www.osce.org/cio/109266?download=true(Switzerland) and http://www.osce.org/cio/134801?download=true(Serbia)

[114] "Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna", available at: http://www.osce.org/cio/126475

promoting its CBMs[115] but also introducing for the first time a simulation-based discussion among various stakeholders from the participating states[116].

Finally, another opportunity for the OSCE to work on cybersecurity issues are its Field Operations (FOs). To that end, the OSCE Mission to Serbia, in cooperation with DiploFoundation and supported by the Geneva Centre for the Democratic Control of Armed Forces (DCAF) organised a series of events in 2015 aiming to support the institutions of the Republic of Serbia towards developing an efficient multistakeholder national framework for cybersecurity[117]. The objective of the project was to gather representatives of relevant national institutions, companies, and organisations, in order to discuss and agree basic principles and recommendations for developing a strategic framework, and primarily a national centre of response to cyber-incidents (CERT) and a national multistakeholder body for cybersecurity issues.[118] Following up on these efforts, the OSCE Mission to Serbia has decided to extend its support and invest further efforts and funds in cybersecurity on two levels: on the one hand, it will continue supporting the creation of the proper legislative, the strategic and institutional set-up on the national level, whilst on the other it will contribute to increase the understanding of risks and threats (both for citizens and institutions) emanating from cyberspace. These activities will be organised throughout 2016 and 2017 and will be supported within the scope of the larger project related to security sector reform, implemented by the OSCE mission to Serbia and funded by the Swedish government. First activity of this type was publication of the "Guide through information security in the Republic of Serbia", aiming to provide basic guidelines for further steps in the process of comprehensive regulation of the area of information security in Serbia.[119]

Apart from the OSCE FO in Serbia, the Macedonian-based OSCE Mission to Skopje has also organised one pilot activity related to cybersecurity in the scope of its trans-national threats-related project umbrella. The activity aims to aid the Macedonian Directorate for Security of Classified Information (previous National Security Agency) in drafting and implementing a Risk Assessment Methodology from cybersecurity/information security perspective tailor made for each state institution handling classified information. The pilot project aims to contribute to improving the general situation related to cybersecurity in Macedonia.

There are no records of other OSCE FOs in the Western Balkans embarking on the cybersecurity-related topics.

5.5 The International Telecommunication Union (ITU)

The ITU is the most active organisation dealing with cybersecurity at the international level. It has produced a large number of security frameworks, architectures and standards.[120] During the second phase of the World Summit on the Information Society in Tunisia, 2005, the ITU was identified as the sole facilitator of the "Action Line C5: Building confidence and security in the usage of ICTs" and as such was tasked by global leaders to coordinate cybersecurity efforts at the global level. In line with this new role, and in accordance with other decisions of the ITU Membership, the Global Security Agenda (GCA) was launched by the ITU Secretary-General in 2007 as the ITU framework for

[115] Available at: http://polis.osce.org/events/details?item_id=4284&lang_tag=EN&_ru=%2F
[116] Available at: http://www.diplomacy.edu/calendar/simulation-exercise-during-osce-chairmanship-event-belgrade
[117] "Serbia's efforts to respond to cyber security threats", available at: http://www.osce.org/serbia/170361
[118] Result publication is available at: https://issuu.com/diplo/docs/ka_nacionalnom_okviru_za_sajber-bez(in Serbian)
[119] The Guide is available at: http://www.osce.org/serbia/272171
[120] Jovan Kurbalija, "Introduction to Internet Governance", 6th edition, page 67, DiploFoundation, available at: http://www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf

international multi-stakeholder cooperation in cybersecurity aimed at building synergies with current and future initiatives and partners towards a safer and more secure information society.[121] The GCA adopted the so-called holistic approach, with five main areas of action. For the purpose of this research, the most important is its fifth 'pillar', namely International Cooperation.

In the scope of this pillar, the ITU has paired in 2008 with a consortium of institutions and organisations called International Multilateral Partnership Against Cyber Threats (IMPACT). The mandate of this unique alliance is to "provide an open partnership platform for international cooperation between governments, industry leaders, academia and law enforcement agencies in order to facilitate the establishment of cybersecurity strategies and critical infrastructure protection, to enhance coordination and cooperation in securing cyberspace"[122]. The collaboration thus pairs industry experts, academia, international bodies, think tanks, which are part of IMPACT's global alliance and which have the know-how, i.e. expertise, technology, skills, resources and experience in delivering top notch cybersecurity related services to some of the 193 ITU Member States. The IMPACT Global Headquarters was officially opened in 2009 upon a 13 million USD grant from the Malaysian Government in Cyberjaya and today it is the home of various ITU-IMPACT activities. The ITU is facilitating the implementation process, managing communication and needs assessment with Member States (MS) and coordinating with IMPACT, to ensure effective delivery of the services provided.[123]

Albania, Bosnia and Herzegovina, Croatia, Montenegro and Serbia are all partner countries of the ITU-IMPACT alliance[124], however only Montenegro has managed to benefit significantly from this partnership to date. Namely, the involvement of the alliance in the region dates back to 2010, when it organised a readiness assessment workshop in Belgrade in relation to establishing n-CIRTs for Serbia, Bosnia and Herzegovina, Montenegro and Albania. In 2012 the same activity was conducted for Macedonia in Skopje. The Montenegrin n-CIRT was created in 2011 as a direct result of the mentioned assessment and with the assistance of the ITU-IMPACT alliance[125]. The alliance then offered capacity-building exercises for representatives of different Government agencies – two representatives from Montenegro attended the 7 days-long training "Developing and Implementing a CIRT team" in IMPACT's HQ in Malaysia, whilst IMPACT experts held a 10 days-long Incident report training specifically designed for 12 Montenegro representatives.[126]

The ITU-IMPACT alliance offers a whole range of technical, non-technical and capacity building related services. Apart from assistance to the creation of national CIRT, the alliance has also been active in organising cyber drills. The first pan-European cross-border cyber drill in Europe organised by the ITU was in Bulgaria in 2012[127] with eight actively participating countries (Montenegro being one of them) and Albania and Croatia from the region among eleven observing countries. The first

[121] Available at: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
[122] Available at: https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf
[123] *ibid.*
[124] Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Status_ITU_IMPACT.pdf
[125] The legislative prerequisite for the establishment of the national CIRT was signing the Administrative Agreement between the Government of Montenegro and the ITU, which occurred on July 29, 2011. More information is available at: http://goo.gl/xsJcgX
[126] *ibid.*
[127] Available at: https://www.facebook.com/notes/impact/itu-impact-holds-first-ever-pan-european-cross-border-cybersecurity-drill/10151297441253023/

ever cross-border cyber drill in the Western Balkans was organised in Montenegro in 2015, in cooperation of the ITU-IMPACT with the Government of Montenegro.

The ITU-IMPACT's considerable assistance to developing Montenegro's cybersecurity capabilities was also extended to the legislative and strategic framework – in cooperation with this alliance, a number of documents were drafted: an Assessment Report on the state of cybersecurity in Montenegro, a Strategy of establishing the National CIRT in Montenegro, an analysis of the Critical Information Infrastructure in Montenegro (2012), which then led to the drafting and adoption of the Methodology of identifying Critical Information Infrastructure (CII) and the Action plan for its implementation.

Finally, it is worth mentioning that the ITU published a National Cybersecurity Guide in 2011. The guide aimed to serve as a reference document for the creation of any national cybersecurity strategy. However, its reach is somewhat undermined by the fact that it relies entirely on the Global Cybersecurity Agenda, adopted by the ITU in 2008. Still, in cooperation with some of the most important international organisations and representatives of the industry, think-tanks and academia, the ITU has undertaken a project to create the so-called "Reference guide" as "a single resource for any country to gain a clear understanding of the purpose and content of a national cybersecurity strategy and how to develop one" and to map "existing relevant models and resources as well as offer an overview of the assistance available from various organisations".[128]The Guide is expected to be available in late 2016, and could serve as an important resource for the Western Balkans countries in the creation and evaluation of their cybersecurity strategies.

[128] Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

6 Existing regional security mechanisms and opportunities

Many regional organisations were initiated and funded by European and international partners as a means of preventing future conflicts through dialogue and activities in the field of security and economic development, among others. Even though not many of them seem to be active in the area of cybersecurity, it is important to explore the opportunities for this, and suggest which organisations might further invest in that direction. This chapter reviews the most important regional organisations and initiatives in the SEE which are, or might be relevant for cooperation among the countries of the Western Balkans, through which specific actions in the area of CS/IS were implemented or could be implemented in the future, as well as particular relevant projects.

6.1 The South-East European Cooperation Process (SEECP)

Launched by the SEE countries on Bulgaria's initiative at the Foreign Affairs Ministerial in Sofia in 1996, the SEECP was created to represent a unique "voice of the region" with the goal of establishing a cooperation framework for developing neighbouring relations and securing stability in the region.[129] The SEECP has a rotating Presidency, annually switching between its 12 member countries: Albania, Slovenia, Bosnia and Herzegovina, Bulgaria, Greece, Croatia, FYR Macedonia (Macedonia), Moldova, Romania, Serbia, Montenegro and Turkey.[130]

The highest strategic political document of the SEECP is the Charter on Good-Neighbourly Relations, Stability, Security and Cooperation in the SEE (The Charter), adopted in 2000. The Charter outlined the goals of the SEECP: Enhancement of political and security cooperation; Fostering economic cooperation; Enlargement of cooperation in the fields of human dimension, democracy, justice and combating illegal activities. The establishment of the Regional Cooperation Council (RCC), in 2008, laid the foundations for region-driven cooperation in the SEE, with SEECP as the main political forum, while the RCC is functionally linked to the Process representing its institutional and logistical support. The SEECP also fostered parliamentary cooperation in the SEE by establishing the SEECP Parliamentary Assembly in 2014.

In 2008, the SEECP members' Ministers of Home Affairs signed a **Common Declaration Regarding the Strengthening of Cooperation in Combating Cybercrime**[131] in Chisinau. In its 12 points, members agreed to step up the efforts on the national and regional level in combating cybercrime by developing more effective mechanisms of cooperation, improving the national legal frameworks and increasing the use of international and regional organisations and initiatives in the process of fighting cybercrime. There are no reports that imply that further efforts, made by the SEE governments, were a direct consequence of this declaration. Nevertheless, the Declaration represents a solid and broad basis for possible future SEECP activities in the cybersecurity field.

Moreover, on 25 June 2014 the **SEECP Bucharest Summit Declaration**[132] was signed. The Heads of States/Governments of the South-East European Cooperation Process (SEECP) stressed the importance of strengthening cooperation in the field of cybersecurity, one of the most important challenges the region is facing, as it was underlined on the occasion of the Regional Conference on

[129] Available at: http://rspcsee.org/en/pages/read/about-seecp
[130] Since 2014 Kosovo* is recognized as a member of the Process, in accordance to the Agreement on the Regional Representation and Brussels Agreement.
[131] Available at: http://www.rcc.int/docs/72/common-declaration-of-seecps-ministers-of-home-affairs-regarding-the-strengthening-of-cooperation-in-combating-cybercrime
[132] Available at: http://www.mae.ro/sites/default/files/file/pdf/2014.06.25_summit_declaration.pdf

Cyber Security "The impact of the global cybernetic threats – developments and prospects at regional level" organised on 23 June 2014, in Bucharest. The declaration clearly states that cyber threats pose one of the most important challenges the region is facing and that strengthening regional cooperation in this field is of utmost importance.

Having in mind that the SEECP operates on the highest governmental level,[133] only general policy directing can be expected on its agenda. As the SEECP chairmanship gives the opportunity for the chair country to set the agenda for the next year, 2016/2017 could be an opportunity for the next chair (Croatia) to further instigate regional cooperation in the CS field. Bulgaria held the latest, 20th SEECP chairmanship (July 1, 2015 – June 30, 2016), but its agenda was primarily focused on the refugee/migration crisis, energy and transport. The next chair will be Croatia.

6.2 The South-East European Cooperation Process Parliamentary Assembly (SEECP PA)

Established in Bucharest in 2014 by institutionalising the SEECP Parliamentary Dimension, the SEECP PA is linked to the SEECP as an international cooperation platform of the states of the SEE region, but is separate from the SEECP governmental dimension. The unique nature of the SEECP PA is that it is a format initiated by the parliaments themselves.[134] The SEECP PA annually gathers from 3 to 5 national parliament representatives of the member states, including the speaker of the house.

The SEECP PA has set broad regional cooperation goals, among which are initiating the exchange of experiences in the field of legislation and its harmonisation with the EU acquis, cooperation in the field of security, encouraging, following and monitoring the realisation of the goals and priorities defined by the rotating SEECP Presidency and the Regional Cooperation Council, strengthening the dialogue with the civil society in the region and intensifying diplomatic activities of the parliaments and establishing links with the regional, European and international organisations, institutions and foundations.

In its **Report on Opportunities for Cooperation in the Field of Justice**[135] from 2015, the SEECP PA clearly categorised organised cybercrime as the significant new regional threat. The Report stresses that the success of the struggle with cross-border organised crime depends on a sophisticated strategy and international cooperation, and commends existing regional initiatives, such as The South-East European Prosecutors Advisory Group (SEEPAG) and The South-East European Law Enforcement Center (SELEC), as good examples of such practice.

The Report recommends mapping the priorities and drafting joint proposals for upgrading coordination and developing integrated action for combating cross border organised crime. Therefore, it could serve as the basis for future proposals of wider CS cooperation. Proposals for more specific judicial cooperation within the CS field could be pursued through national parliament representatives, especially bearing in mind the Croatian chairmanship (2016 – 2017) and the access that the EU members of the SEECP PA have in the European Parliament.

---

[133] Highest level: Annual meetings of the Heads of State and Prime Ministers - forum for recommendations and discussions; Second level: Annual meetings of Foreign Ministers entrusted to manage the implementation of common objectives; Third level: The Committee of Political Directors consisting of the political directors of Foreign Ministers of participating countries, meeting quarterly; Fourth level: ad hoc sectorial ministers meetings (in the fields of economy, trade, telecommunications, energy, interior affairs, culture).

[134] Available at: http://rspcsee.org/en/pages/read/seecp-parliamentary-assembly

[135] Adopted by the SEECP PA General Committee on Justice, Home Affairs and Security Cooperation, on February 10, 2015, in İstanbul, available at: http://rspcsee.org/assets/userfiles/2nd%20Plenary%20Session/Report%20JHS%20GC%20_10%2002%202015_-_005_.pdf

6.3 The Regional Cooperation Council (RCC)

The RCC is a regional cooperative framework for countries of the SEE that serves as the operating arm of the SEECP, and is under its political guidance. The RCC is the formal successor of the Stability Pact for South-Eastern Europe, a regional umbrella institution established in 1999 with the aim of strengthening peace, democracy, human rights and the economy in the countries of South-Eastern Europe. In 2008, the Stability Pact was replaced by the more regionally driven RCC. The RCC participants comprise of 46 countries, organisations and international financial institutions. The organisation has a Secretariat based in Sarajevo, Bosnia and Herzegovina, headed by Secretary General Goran Svilanović[136].

The core element of the RCC's work is the South-Eastern Europe 2020 Strategy[137] (the Strategy). Adopted in November 2013, the Strategy's primary focus is economic development. The Strategy mostly refers to ICT in the part concerning the development of digital society[138]aiming to achieve faster regional economic growth. Strategy foresees several actions within this dimension: the development of regional broadband infrastructure, cross-border eServices, IT training and support to the ICT driven public sector innovation. The implementation of these actions is to be supervised by the e-SEE initiative. The cybersecurity issues are not explicitly mentioned in the Strategy, but they are implied indirectly within the "Smart Growth" and "Governance for Growth" pillars of the Strategy, more precisely its "Digital Society", "Justice" and "Effective Governance" dimensions. The Strategy is implemented via its action plans or "Strategy and Work Programmes".

The organisation currently operates under its Strategy and Work Programme 2014-2016 (SWP 14-16)[139] which is the main document guiding its short-term work in meeting the Strategy framework goals. The cybersecurity aspects of this Programme can be found within the activities foreseen by the "Government for Growth" section. The Programme designates that the RCC should, as a permanent activity, support the strengthening and organisation of the existing informal networks of experts dealing with highly specialised topics like: frauds, cybercrime, identity thefts, confiscation and recovery of assets to establish a safer environment for the businesses in SEE. There are no actions foreseen by the Programme for the Strategy Action 4 within "Digital Society" dimension of the "Smart Growth" pillar on advancing of network security and data protection across the region of SEE.

An important aspect of the RCC Strategy and Work Programme (SWP) 2014-2016 is streamlining of the Regional Initiatives and Task Forces (RI and TF).[140] The RCC has ties to a number of such initiatives in the domain of Security Cooperation, but only a few of them began to pursue cybersecurity issues, and none of them are exclusively committed to those issues. CS-tackling initiatives/organisations are SEENSA, SEEMIC, RESPA, RACVIAC, SEPCA, SELEC and eSEE – all are elaborated in more detail below.

It is noteworthy to mention that the RCC Secretariat initiated a direct cooperation with the Council of Europe in the field of Cybercrime. The Secretariat's experts attended the OCTOPUS Interface

[136]Svilanović took office on 1 January 2013 and was re-elected in 2015 to remain at the position until the end of 2018.
[137] Available at: http://www.rcc.int/files/user/docs/reports/SEE2020-Strategy.pdf
[138]RCC.South East Europe 2020. 3.2. Smart Growth pillar, Dimension F „Digital Society". November 2013.
[139]RCC. Strategy and Work Programme 2014 – 2016. April 2013, available at: http://www.rcc.int/files/user/docs/reports/RCC-Strategy-and-Work-Programme-2014-16-text.pdf
[140] In order to pursue its goals the RCC establishes relationships with relevant regional co-operation taskforces and initiatives in SEE, using them as a relevant source of information and analysis in the wider process of identifying gaps and opportunities in regional cooperation. The RCC assists the taskforces/initiatives in gaining access to regional and international political, technical and financial support required to fulfil their objectives.

Conference – Cooperation against cybercrime, in 2009. On this occasion, the RCC and CoE representatives identified complementarities and synergies between the 2nd phase of the CoE Global Project on Cybercrime and the "RCC Cybercrime Project Idea".[141] However, no cybercrime project has been developed by the RCC to date.

The RCC itself had no direct activities concerning CS issues, and it is likely that it will have even less of a focus on security in the coming years; nevertheless it remains a very useful framework for facilitating regional mechanisms committed to the cooperation and development of the goals outlined in the Strategy. Actions concerning CS could be specified and stressed within the new Strategy and Work Programme that is expected to be adopted in late 2016, right after the mid-term evaluation of the Strategy implementation. It is important to keep in mind that these actions must fall within existing objectives of the "Justice" dimension, and to some extent of the "Effective Public Services" and "Digital Society" dimensions. There is an opportunity to advocate for more actions concerning Action 4 of Dimension F "Digital Society" within the "Smart Growth" pillar of the Strategy[142], as there were no actions for it within the present Programme. The RCC can also be a good venue to initiate public-private partnership projects in the CS field via the SEE PPP Network, operating under the auspices of the RCC.

6.4 The South-East European National Security Authorities (SEENSA)

In 2011, the RCC co-organised the first meeting of the South-East European National Security Authorities (SEENSA)[143] to discuss the practical aspects of a regional cooperation concerning the functioning of the system for the protection of classified information. The SEENSA soon broadened its scope as it identified the need to regulate cyber defence at the regional level in line with security policies implemented by the EU and NATO.[144] The SEENSA gathers the heads of the national security authorities from Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Kosovo*, Macedonia, Moldova, Montenegro, Serbia and Slovenia[145].

One of the first steps in tackling the issue of CS was taken by setting up the **SEENSA Thematic Working Group for Cyber Defence**[146]in 2014, coordinated by the Director of the Office of National Security Council and Classified Information Protection of Serbia, with the support of his counterparts from Bosnia and Herzegovina, Bulgaria, Montenegro, Moldova and Slovenia. Besides this TWG, the SEENSA has created three more groups on Security agreements, the Training of personnel with access to classified information and the Industrial security.

In its five meetings,[147] SEENSA members were mainly focused on reviewing the achievements and conclusions made by the Thematic Working Groups. These meetings were used to discuss the future cooperation between the NSA and the States of the region on the issues of sharing the best experiences and legal harmonisation in all areas of information security.

---

[141] Available at: http://www.rcc.int/download/pubs/RCC-Annual-Report-2008-2009.pdf/a5883c4d7cdc80b7cd79fd6e49ffc9b5

[142]RCC SEE2020 Strategy. p22 – Dimension F "Digital Society", Action IV: Advancement of network security and data protection across the region of the SEE

[143] The conference was held in May 2011 and was fully supported by the NATO Office of Security and the EU General Secretariat of the Council. Available at: http://www.rcc.int/articles/79/seensa-new-regional-format-of-advanced-protection-of-classified-information

[144] Available at: http://www.rcc.int/articles/137/trust-and-confidence-prerequisites-for-advancing-protection-and-exchange-of-classified-information-in-south-east-europe

[145]Romania, Turkey and Greece missing from membership.

[146] Available at: http://www.dbki.gov.mk/?q=node/400

[147] The SEENSA meetings so far: 2011 - Sofia, Bulgaria; 2012 - Kranj, Slovenia; 2013 - Durres, Albania; 2014 - Sarajevo, Bosnia and Herzegovina; 2015 - Skopje, Macedonia; May 2016 - Montenegro.

One of the more conclusive results of the cooperation is the initiative from 2014 to develop a theoretical regional cyber defence model as the strategic and legal framework for cooperation of all the SEENSA members in the field of CS/IS, and also to organise the training of the NSA representatives for communication and information security (CIS Security Authorities) and to prepare the strategic and legal framework. No supporting documents were available on this initiative to date.

6.5 The South-East European Military Intelligence Chiefs (SEEMIC)

The South-East European Military Intelligence Chiefs Conference (SEEMIC) is a forum of high level military intelligence officers from the region that allows for networking, building relationships and strengthening trust as a basis for furthering cooperation in the intelligence area. SEEMIC was created under the patronage of the RCC in 2009 and gathers national military intelligence representatives from twelve South-East European countries – Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Moldova, Montenegro, Romania, Serbia, Slovenia, Macedonia and Turkey.

The SEEMIC has held eight meetings so far[148]. There is insufficient evidence that there are more concrete actions taking place concerning CS/IS as the result of these meetings, but it is worth noting that its sixth meeting, held in 2014 in Skopje, Macedonia, was focused on cyber-threats as a rising security issue in the SEE. Participants stressed the importance of the cooperation on this issue and the necessity for a joint approach to modern security challenges.[149] As an example of good practice, members of the Military Academy of the Republic of Macedonia mentioned the signing of the Memorandum of Cooperation with the Initiative for Cyber-Security of the Monterey Institute of International Studies, USA, as well as holding the regional round table for cybersecurity, which was held in cooperation with NATO and Norwich University from the USA.

SEEMIC is looked upon as "one of the most important and successful regional initiatives in South-East Europe"[150] and is continuously supported by the RCC, NATO and the EU, whose representatives regularly attend the meetings. Keeping in mind that the SEEMIC has no reported activities within the CS field, and also the closed nature of military intelligence, it is hard to foresee the opportunities for cooperation within this initiative, yet it is likely to expect that it could push for more cyber defence topics on its agenda in future.

6.6 The e-SEE Initiative

The Electronic South Eastern Europe (e-SEE) Initiative was initiated in 2000 with a goal to integrate SEE countries into the global, knowledge-based economy by regionally supporting the development of Information Society. Its Secretariat is hosted by UNDP Country Office in Bosnia and Herzegovina, and e-SEE received valuable guidance and support from UNDP, European Commission, and the UN Economic Commission for Europe (UNECE).

Actions undertaken by e-SEE Initiative are complementary to the effort of drawing SEE closer to EU action plans for Information Society development expressed in the Digital Agenda for Europe. The RCC worked closely with e-SEE in implementing the Initiative adopted e-SEE Agenda for the development of Information Society (2002-2007) and e-SEE Agenda Plus in 2007 (2007-2012). e-SEE was also designated to be the responsible regional structure for implementation of the strategy

[148] SEEMIC meetings so far: 2009 – Bucharest, Romania; 2010 – Belgrade, Serbia; 2011 - Sarajevo, Bosnia and Herzegovina; 2012 - Sofia, Bulgaria; 2013 - Split, Croatia; 2014 - Skopje, Macedonia; 2015 – Thessaloniki, Greece, May 2016 - Moldova
[149] Available at: http://goo.gl/N8z2R3
[150] Available at: http://www.rcc.int/news/99/south-east-european-military-intelligence-chiefs-meet-in-sofia

measures of the "Digital Society" dimension of SEE2020 Strategy. e-SEE tackles the issue of CS only in the context of development of information society for the benefit of the economic growth. Since the implementation of the Agenda Plus, however, there is no indication that the Initiative is still active.

6.7 The Centre for Security Cooperation (RACVIAC)

Centre for Security Cooperation (RACVIAC)[151] is an international, independent, non-profit, regionally owned, academic organisation based in Croatia. Established in 2000, its mission was promoting confidence, cooperation and security building measures within the SEE. Reacting to the changing needs of the SEE countries, a new Agreement on RACVIAC was signed in 2010 that broadened its scope of activities to security sector reform and international and regional cooperation with a focus on Euro-Atlantic Integration.

RACVIAC was established by eight member states: Albania, Bosnia and Herzegovina, Croatia, FYR Macedonia, Montenegro, Romania, Serbia[152] and Turkey. RACVIAC is accountable to its steering committee - political decision making body, the Multinational Advisory Group (MAG).

RACVIAC recognised the importance of CS in 2010 when it started holding regional conferences on various CS issues such as: CS strategies, the impact of cybercrime on economy, personal data protection, cyber resilience, etc. Besides conferences, RACVIAC also held research workshops for regional CERT representatives, and a NATO Advanced School on Cyber Defence. These events gathered experts and decision makers from the member states, associate member states and from other international and regional organisations. CS activities are operating under RACVIAC's International and Regional Cooperation Pillar.

In 2014/2015 RACVIAC established close cooperation with the Military Academy "General MihailoApostolski" in Skopje in the area of CS. Two CS events were jointly held in 2015with the support of the Federal Republic of Germany. These events tied all RACVIAC CS activities into a project effort to develop cyber resilient societies within the SEE. One of the project objectives is to initiate and develop a network of dedicated personnel, ready to improve regional cooperation in the context of building cyber resilient societies in the SEE. This project is still ongoing in 2016.[153]Also, RACVIAC has managed to obtain funds from the NATO Science for Peace programme, and will hold Advanced Training Course titled "Building a Cyber Resilient Society in South Eastern Europe" in October 2016[154].

Having in mind that RACVIAC has very strong relations with the relevant ministries from its member states[155], through its CS activities had gathered more than 200 experts from the region, has regular CS activities and support, and is committed to further develop its CS programme, it could serve as one of vital pillars of future regional cooperation within the CS field, at least on the technical/expert level.

6.8 The South-East Europe Cyber Security Centre (SEECSC)

The SEECSC is a cybersecurity research and development centre, based in Sarajevo, and established as an organisational unit at the American University in Bosnia and Herzegovina. Its mission is to

[151] Formerly *Regional Arms Control Verification and Implementation Assistance Centre* (2000-2010) More information available at: http://www.racviac.org/

[152]Kosovo* was invited in October 2014 to participate on a permanent basis, at all levels and on equal terms in all activities and meetings.

[153] Available at: http://www.racviac.org/downloads/2016/IRC-O1-P-16_overview.pdf

[154]Available at: http://www.racviac.org/downloads/2016/IRC-O6-P-16_agenda.pdf

[155] Available at: http://racviac.org/news/index.html

deliver quality education, research and services to overcome the region's challenges of securing and protecting cyberspace. Its primary goal is to bring valuable projects to enhance the region's capabilities in cybersecurity and to further cybersecurity-related research and education activities in the region. The SEECSC has formed partnerships with BIH government institutions[156], international institutions and think-tanks[157], and universities[158].

In cooperation with RACVIAC, in 2014, the SEECSC organised an international conference "Ensuring personal data protection while securing cyber space: Challenges and perspectives for the South-East European Countries" in Sarajevo. The participants and lecturers included representatives from all over SEE, USA, the EU, and international organisations, with around 150 participants in total. The conference aimed at promoting the exchange of information, transfer of knowledge, views, ideas and standards regarding data protection.

In 2012 the SEECSC parent organisation - American University in Bosnia and Herzegovina, organised a successful international conference under the title "Western Balkan Security, Technology and Education: The challenges within cyber infrastructure", to identify current challenges in addressing cybercrime in the region and potential means of coordination in the field of cybersecurity. Seven Ministers of Interior/Security from the Western Balkans and Turkey agreed on the Joint Statement[159].

There is no further reported activity, and it seems that after the 2014 conference, the organisation ceased to work actively.

6.9 The Southeast European Law Enforcement Center (SELEC)

SELEC is the regional organisation devoted to prevention and combating trans-border crime through regional cooperation and coordination. It is the successor to the SECI Regional Center for Combating Trans-border Crime since 2009. The SELEC is organised under the auspices of the SEECP. The SELEC member states are Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Macedonia, Greece, Hungary, Moldova, Montenegro, Romania, Serbia and Turkey.

SELEC serves as an effective mechanism with significant potential for cooperation within CS. The SELEC's operational work is organised through eight Task Force groups whereas one of the groups is committed to financial and computer crimes[160], with the subgroup dealing with cybercrime based in Romania. This TF organised a number of regional meetings and conferences focused on cybercrime and CS issues, which were attended not only by member states, but also international partner organisations (INTERPOL, EUROPOL, SEEPAG…) and stakeholders from the private sector. Furthermore, the SELEC is annually awarding regional actions and operations against crime, and in 2015 it awarded a successful joint Macedonian and Serbian law enforcement computer crime operation.

The SELEC has three active projects, but none fully focused on cybercrime issues. The OCTA SEE project is dedicated to the development of strategic, future-oriented analysis called Common Threat Assessment on organised Crime for the SEE; the document has a four yearcycle, the last one

[156] Presidency, Parliamentary Assembly, Ministry of Security, Ministry of Defence and Ministry of Foreign Affairs
[157] UN, RACVIAC, Peace Support Operations Training Centre (PSOTC), The George C. Marshall European Center for Security Studies, and Institute for Cultural Diplomacy
[158] Western Kentucky University (USA), West Virginia University (USA), Northeastern University (USA), George Mason University (USA), SALEM State University (USA), Kafkas University (Turkey), Nigde University (Turkey), Istanbul Aydin University (Turkey) and AMITY University (India)
[159] Available at: http://seecsc.org/JointStatement.pdf
[160] Available at: http://www.selec.org/p261/Financial_and_Computer_Crime_Task_Force

beingfor the period of 2013 to 2016 – unfortunately it is not available on-line[161]. Project activities are financially supported by the US, the OSCE and the EU. It might be worth noting that Romania, Bulgaria and Macedonia seem to be more active as members than other countries.

6.10 The South-East European Prosecutors Advisory Group (SEEPAG)

The SEEPAG[162] is an international mechanism of judicial cooperation, formed in 2003 by the countries of the SEE region with the expressed intention of building further support for the SELEC in facilitating judicial cooperation in significant trans-border crime investigations and cases. The SEEPAG is composed of the national representatives of member states – high ranked experienced prosecutors or judges.

Under the Croatian chairmanship (2011), the SEEPAG organised a conference on investigating and prosecuting cybercrime, with the help of US experts and the SELEC. In 2015, members of the SEEPAG participated in the CoE meeting under the framework of the CyberCrime@EAP II project on Improving International Cooperation on Cybercrime in the Eastern Partnership region.

Due to the fact that both organisations are very active, have legal status, good relations with the RCC and the SEECP, experience with projects focusing on trans-border crime prevention, and that they include all the SEE countries, the SELEC and the SEEPAG could pose as a good framework for regional cooperation within the field of cybercrime.

6.11 The Southeast Europe Police Chiefs Association (SEPCA)

The SEPCA is an association that gathers the police chiefs of its member states, dedicated to building public security in the SEE, through co-operative police services. The SEPCA members are: Albania, Bosnia and Herzegovina, BIH – RepublikaSrpska, Bulgaria, Croatia, Macedonia, Moldova, Montenegro, Romania and Serbia.

The SEPCA was created in January 2002 and has a secretariat in Sofia. The Association is steered by the Executive Committee. The SEPCA's activities were largely supported by the Canadian Government, the Swiss Agency for Development and Coordination (SDC) and the Geneva Centre for Democratic Control of Armed Forces (DCAF).

The SEPCA had only one project concerning CS - “Strengthening regional capacities in the fight against cybercrime”[163]. The project's goal was to increase security and confidence in information and communication technologies (ICT) in the SEPCA region and to improve the capacity of computer crime research in the police service of the members the SEPCA. Montenegro was designated as the member responsible for implementation. There are no reports of the activities and the impact of this project.

The SEPCA Strategy & Action Plan (2011-2013) does not recognise cybersecurity as an important issue, no strategy document can be found for the period after 2013. Besides one report on the SEPCA meeting in 2015, it seems that since the end of 2013, there was no activity within the SEPCA. Although police chiefs in the SEE countries have influence that could help instigate regional police CS cooperation, the inactivity of this initiative in the last two years, and the asymmetry of activity of its members, is a strong signal that the initiative has significant weaknesses.

[161] Information about the initiative is available at: http://www.selec.org/p460/OCTA+SEE
[162] Available at: http://www.seepag.info/
[163] Available at: http://www.sepca-see.eu/projects/current-projects

6.12 Police Cooperation Convention for Southeast Europe (PCC SEE)

Another regional organisation that has recently included CS in its portfolio is PCC SEE. This organisation is not created under the auspices of RCC, it is rather a genuine regional initiative of the Ministers of Interior of seven SEE countries[164]. The Convention was signed in 2006 in Vienna and ratified in 2007, when it entered into force. In addition, from 2008 – 2012 Bulgaria, Austria, Hungary, and Slovenia acceded to the Convention. The Convention "…envisages modern forms of cooperation among the Contracting Parties (such as joint threat analysis, liaison officers, hot pursuit, witness protection, cross-border surveillance, controlled delivery, undercover investigations to investigate crimes and to prevent criminal offences etc.) […] and its aim is to adopt Schengen standards for the improvement of strategic police collaboration in the region".[165]
The Contracting Parties are strongly supported primarily by Switzerland, the European Commission, DCAF and Liechtenstein. The PCC SEE Secretariat is located in Slovenia and is hosted and supported by DCAF. In October 2016, the PCC SEE will hold its first ever workshop on ICT security in Belgrade, which might mean that its Contracting Parties aim to engage further in this area, particularly from the police cooperation point of view.

6.13 The Regional School of Public Administration (ReSPA)

The ReSPA was formed in 2010 as the organisation committed to boosting regional cooperation in the field of public administration, strengthening administrative capacities as required by the European integration process, and developing human resources in line with the principles of the European Administrative Space.[166] Members of the ReSPA are Albania, Bosnia and Herzegovina, Croatia, Macedonia, Montenegro and Serbia. The ReSPA's offices are located in Danilovgrad, Montenegro.

Even though the ReSPA is not explicitly focused on cybersecurity, it tackles those issues through their impact on the development of eGovernment. The ReSPA held training on Internet governance and enforcement of intellectual property rights (2014), developed comparative studies on the development of eGovernment in the SEE (2013), and the use of IT for corruption (2013). The ReSPA also organised conferences and meetings of government representatives and the private sector on all the aspects of development of eGovernment and Open Government, focusing on the potentials of public-private partnership in this field.

The RCC has developed good relations with the ReSPA and counts on it as a place for joint regional trainings in achieving regional strategic goals[167]. ReSPA is continuously supported by the EC. Its activities show that working under the "strengthening capacities of public administration" umbrella could be one important way to tackle CS issues.

6.14 The Central European Initiative (CEI)

The CEI is a regional intergovernmental forum committed to supporting European integration of its Member States via inside coordination and cooperation with the European Union (EU), international and regional organisations, and the private and civil sectors.[168] The CEI actions in the area of

[164] Albania, Bosnia, and Herzegovina, Macedonia, Moldova, Montenegro, Romania and Serbia
[165] Available on: http://www.pccseesecretariat.si/index.php?item=9&page=static
[166] Available at: http://www.respaweb.eu/
[167] Available at: http://www.rcc.int/pages/36/rcc-and-regional-initiatives-and-task-forces-in-south-east-europe
[168] Available at: http://www.cei.int/content/mission-objectives

cybersecurity are only a by-product of its activities in implementing the Digital Agenda of the Europe 2020 Strategy,[169] which has "Strengthening online trust and security" as one of its seven pillars. Even though the CEI did not implement any Information Society projects concerning CS to date, it has two available fund lines for implementing projects within this niche: the CEI Cooperation Fund[170] and the CEI Know-How Exchange Programme (KEP)[171]. The CEI currently operates under the Plan of Action 2014-2016[172], while the new plan is expected to be adopted at the end of 2016. This could be an opportunity for the SEE countries to influence incorporating the EU Digital Agenda CS priorities into the Plan.

6.15 The South-Eastern Europe Defence Ministerial Process (SEDM)

The SEDM Process[173] is an initiative that gathers defence ministers from the SEE region, with the goal of promoting regional cooperation and good neighbourly relations, strengthening regional defence capabilities and establishing links that facilitate integration into Euro-Atlantic institutions. Participating members are Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Georgia, Greece, Italy, Macedonia, Montenegro, Romania, Serbia, Slovenia, Turkey, Ukraine and the USA.

The SEDM initiative is active in promoting cooperation, either via its annual meetings, long term projects or its sub-initiatives like the SEEBRIG and Deputy Chiefs of Defence (DCHOD) meetings. Unfortunately, CS is not on the SEDM agenda, although in one of the meetings the SEDM recognised cyber-threats (mostly cyber-terrorism) as a rising security issue in the SEE (2014).

The SEDM is currently chaired by Turkey which has a mandate until 2017. Cooperation within the CS field is not on the Turkish chairmanship agenda.

6.16 Projects relevant for the Western Balkans

Cyber Security in Danube Region (CS Danube) was launched in April 2015, with the objective to strengthen trust and cooperation between the security teams CERT/CSIRT, to share their know-how and tools. An integral part of the project represents the strengthening of capacities through training focused on website security. The team CSIRT.CZ that is operated by the CZ.NIC Association acts as the project coordinator. The realisation of the project is supported by the START program of the EU Strategy for Danube region[174]. Partners from Austria, Slovakia, Croatia, Serbia and Moldova take part in the project.

South Eastern European Dialogue on Internet Governance (SEEDIG)[175]is an open, inclusive and informal space for dialogue on Internet governance issues between stakeholders from South Eastern Europe and the neighbouring area. SEEDIG is a sub-regional initiative of the UN Internet Governance Forum. SEEDIG annual meetings are organised in a bottom-up, inclusive and transparent manner, by a multistakeholder group of individuals from the SEE and the neighbouring area, with support from various entities from beyond the region. SEEDIG's first meeting was held in 2015, in Sofia, Bulgaria and the second in 2016 in Belgrade, Serbia, while the Republic of Macedonia will host the 2017 meeting in May, in Ohrid. Cybersecurity, with a diversity of sub-topics, has featured strongly in the

[169] Available at: http://www.cei.int/content/information-society
[170] Available at: http://www.cei.int/content/cooperation-activities
[171] Available at: http://www.cei.int/KEP
[172] Available at: http://www.cei.int/sites/default/files/attachments/docs/Information%20Society%20/502.001-14_plan_of_action_2014-2016_final.pdf
[173] Available at: https://sedmprocess.org/
[174] Available at: http://www.danube-region.eu/
[175] Available at: http://www.seedig.net/

first two meetings, and it is expected that this trend will continue. SEEDIG attracts participants from all stakeholder groups and more than 15 countries in the region.

FIRST[176] is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs. The incident response teams participating in FIRST represent organisations that assist an information technology community or other defined constituency in preventing and handling computer security-related incidents. Out of WB countries only Croatia has two teams participating in FIRST and Montenegro one, but it is expected that, with the emergence of other national CERTs, other countries will join as well.

Organised as one of TERENA (Trans-European Research and Education Networking Association)[177] task force groups, **Task Force Collaboration Security Incident Response Teams (TF-CSIRT/GEANT)**[178] operates as a group for the collaboration of Europe-wide security incident response teams. TF-CSIRT provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination. It maintains a system for registering and accrediting CSIRTs, as well as certifying service standards.[179] The task force further liaises with FIRST, ENISA, European national research and education network (NREN), other regional CSIRT organisations, as well as defence and law enforcement agencies. TF-CSIRT is financed from EU funds, network service subscriptions, projects, membership fees and provisions from administrative, consultancy and training services. Accredited Western Balkan CERTs, with membership in TF-CSIRT, are the Albanian national ALCIRT (listed 2013), Croatian CERT ZSIS (accredited 2009) and national HR-CERT (accredited 2010), Montenegrin national CIRT.ME (listed 2013) and Serbian academic AMRES-CSIRT (listed 2011). TF-CSIRT could serve as a useful framework for technical cooperation of Western Balkan CERTs in knowledge sharing, coordination and skill development. For this to happen, all WB CERTs should apply for membership and pursue accreditation and licensing.

[176] Available at: https://www.first.org/
[177] TERENA joined forces with DANTE in 2014 to become the organisation known as GÉANT. Available at: http://www.geant.org/
[178] Available at: https://www.terena.org/activities/tf-csirt/
[179] Through service called Trusted Introducer (TI), available at: https://www.terena.org/activities/tf-csirt/and https://www.trusted-introducer.org/index.html

7 Conclusion

The European and international legal environment on cybersecurity and information security (CS/IS) provides relevant and comprehensive guidance for WB countries to develop internal legal and operational frameworks. All Western Balkan (WB) countries are formally aligned with the core international mechanisms such as the Budapest Convention, even though some countries still need to work on transposing them into domestic legislation; nevertheless, the very constitutions of the WB countries prescribe that, by accepting such international documents, they became a part of the domestic legislative system. Therefore, there is particular progress with the legal framework for combating cybercrime in all the countries, yet the effective implementation of these mechanisms still remains the challenge, especially on the part of police cooperation, preventing and tracking child abuses and similar crimes, fraud and money laundering, etc., particularly due to the lack of human and financial resources for the established police, prosecutorial and judicial units, which comes as a result of the lack of political interest in actual implementation.

With regards to the EU *acquis* and process of accessing to the EU, the progress with alignment with EU legislation is evident, and most countries started working on or have already enacted core legal acts in the field of CS (though criminal matters mostly) and IS (within specific legislation). However, the strategic framework in CS/IS is mostly missing and the biggest gap is with respect to the legislation in the area of critical infrastructure. Similarly to the CoE-related processes, efficient implementation of CS measures is missing due to a lack of political attention and capacities among implementing institutions. Fast developments in the EU environment, such as with the Digital Single Market, Network and Information Security (NIS) Directive or General Data Protection Regulation (GDPR), could therefore make the WB countries lag behind even more if they do not bring up cybersecurity high on the political agenda. For instance, full harmonisation and implementation of the requirements of the NIS Directive into national practices of Western Balkan countries is a complex process, especially since it emphasises a new approach through private-public partnerships and stronger ties with industry; therefore technical assistance and trainings to help drafting, implementation and effective enforcement of policies in this area are essential. The EU sees digital environment and security among its high priorities, which is not the case with Western Balkan countries which are missing a strategic approach to these areas.

In general, Western Balkan countries are not using the mechanisms that they transposed through legislation. The prime example is criminal legislation in this field, where even though criminalisation of the acts is done in accordance with the international legal framework, there are not sufficient track records, fast international cooperation in regards to investigations, professional capacity in the police units to track and recognise sophisticated hi-tech crimes, etc. Furthermore, while the EU legislation is providing a basis for the enlargement countries to get involved and cooperate with professional organisations at the EU level (like ENISA), such opportunities are not exploited by the WB countries. Finally, the major emphasis in the EU in the area of IS is on public-private partnerships and the great involvement of the IT industry, whereas in the Western Balkan countries this approach is not even on the long run agenda - in part because of the traditionally low interaction of the public sector with other stakeholders beyond mere formalities, and general mistrust between the government and private and non-government sectors.

Most of the international and regional soft-laws - such as those of the OSCE and the UN GGE - require states (even though voluntarily) to invest in setting up national operational mechanisms

(such as contact points and CERTs) and enhance communication among them; increase the readiness of critical infrastructure and share concerns about risks and incidents; establish diplomatic communication and understanding of the matter; in order to be able to act appropriately in case of incidents. More importantly, those frameworks provide venues for political cooperation among countries in the region, especially on the diplomatic and high level which is crucial for developing greater political awareness about the risks and needed regional cooperation. Besides, such frameworks can facilitate cross-professional and cross-institutional communication within and across WB countries. Nevertheless, WB countries are generally missing or have a low profile in these processes; there is a lack of understanding among diplomats of the relevance of cybersecurity, insufficient capacities to understand the area and prepare to respond to risks in the right manner, and lack of communication among various line ministries, in charge of foreign affairs, information society, security, education, economy, etc. - let alone communication with private and non-government sector.

A wider set of global support programmes and resources by international organisations - such as those of ENISA, CoE, NATO or ITU - provide lots of opportunities for building appropriate and efficient legal and operational frameworks, yet only some WB countries have actually used a few of the available resources. For example, Article 24 of ENISA 2004 Regulation and article 30 of the new ENISA Regulation 2013, foresees participation of third countries in case of concluded agreements with the EU Commission and under the condition to apply Community legislation in the field of cybersecurity. Being so, this Regulation is providing opportunity for Western Balkan countries to be part of the ENISA network and to benefit from the expertise already gathered by this important agency through capacity building and sharing of expertise. This is definitely the most important channel for Western Balkan countries to cooperate with EU countries on this matter and to create stronger cooperation among them, which is not explored up to now. Equally important is the huge potential of the joint EU and CoE training programmes offered to all the signatories (and even non-signatories) of the Budapest Convention, which remain underused by WB countries.

Detailed country reviews shows that there is lack of efficient operational mechanisms, capacities and resources that are needed to cope with the growing possibility of cyber-attacks and in most of the cases the organisational aspects still need to be fully established. Cyber capacity building remains a challenge and significant efforts are needed in order to promote a safe, secure and open use of cyberspace in the Western Balkan region. The level of implementation of strategic and legal measures seems to lag behind the formal environment.

First, the progress in formalities is mainly pushed by the EU negotiation requirements rather than thanks to aas a result of political awareness; in fact, a lack of political vision and capacities to comprehend the complexity and importance of cybersecurity - both in terms of the risks to and potentials for the economy and society - result in a lack of a comprehensive and strategic follow-up on action plans and partnerships with other stakeholders. Only Montenegro and Kosovo* have shown a somewhat greater political will to push the cybersecurity agenda - Montenegro for economic reasons, and Kosovo* in order to smartly use the available development aid opportunities.

Second, there is a lack of policy-making capacity among the key institutions in charge of developing and adopting legal and strategic environment - line ministries and the parliamentarians. This can be seen from numerous implementation mistakes, such as overburdening the CERT in Albania with too many tasks while keeping it understaffed and lacking resources, “bureaucratising” operational

responses to cybersecurity threats through concentrating most duties within the Ministry portfolio in Serbia, missing the opportunity to benefit from the expertise and knowledge of the private and civil sectors in the process of policy development and implementation in all countries but Kosovo*, or underusing the available development aid opportunities in most countries.

Third, the capacities and resources (funds, training, travel, human resources, and equipment) of the established operational mechanisms, such as n-CERTs, high-tech crime police units and prosecutor offices, are severely restricted. The efficiency of these bodies - which is sometimes remarkable, as in the case of cybercrime units in Serbia - depends almost entirely on the enthusiasm of individual employees.

Fourth, cooperation with the private sector on cybersecurity matters remains at an early stage of development throughout the region. Few countries, such as Albania and Montenegro, have developed strategic documents on cybersecurity which envisage institutional cooperation with civil society and the private sector in the future. However, none of the countries have established a formal policy dialogue, and even the level of consultations with the private and civil sectors is kept at a minimum. At the same time, there is lack of trust and even motivation of the private and civil sectors in government activities in the field, and each sector - even each actor - seems to be working in closed silos with few interactions beyond individual contacts.

Fifth, there is almost no substantial capacity building or educational programme in cybersecurity policy in any of the countries, except for Montenegro and Bosnia and Herzegovina, which host academic postgraduate programmes. Nevertheless, there are no indications that this capacity is strategically used by the respective governments or other governments in the region.

Lastly, overall cybersecurity culture is not at a remarkable level, and different sectors have varying capacities and interests in cybersecurity; for instance, the banking sector increasingly performs cybersecurity measures, yet indicators still point to many critical vulnerabilities in their systems; electronic communications operators enact stricter security measures in order to protect their networks; operators of critical infrastructure, however, seem to be generally unaware of the risks and entirely left out of the dialogue - moreover, very few countries in the Western Balkans have made any formal steps towards defining what critical infrastructure is, let alone towards operational measures and dialogue with the operators.

All international organisations present and operational in the Western Balkans territory have tackled some of the issues stemming from the emergence of cybersecurity as an issue *par excellence*. For instance, the UNDP, ITU and OSCE have given significant support in different countries in developing strategies or multistakeholder dialogue, or setting up CERTs. Their approaches are, however, different and rarely systematic, whilst the topics they deal with sometimes overlap, thus duplicating the efforts and provoking non-rational budget spending.

On the other hand, since the area of cybersecurity is “policy-in-creation” for all the international organisations active in the Western Balkans, it is not strange that there is no systematic, regional policy on this level. Each of the organisations is interested in some of the issues (which are in line with the organisation’s priorities) and none of them showed the intention of creating a regional policy for developing cybersecurity capacities, legal or institutional frameworks. The most notable example is the ENCYSEC project, which is operational only in some parts of the Western Balkans, and paired with another East European country, for the purpose of acquiring particular EU funds.

There are, however, multiple funding and support opportunities in the region, most notably the EU IPA and Horizon2020 funds, the NATO Smart Defence programmes and the ITU-IMPACT activities. Nevertheless, again only some WB countries have actually used a few of the available opportunities.

The EU IPA funds could be used for enhancing competitiveness and growth in the region, through the role of cybersecurity for e-commerce and protecting the financial market as well as small and medium enterprises (SME), but also for the cybersecurity and IT start-up industry. In particular, the RCC and the ReSPA could play relevant roles since those two institutions are recognised as the focus of IPA II activities; besides, the RCC's SEE Strategy 2020 states that its goal is boosting the ICT industry through empowering SMEs, while the ReSPA is perceived by the IPA II programme as the main capacity-building institution in the region. Horizon2020 projects can, on the other hand, strengthen the cooperation with EU partners thanks to requiring consortia of institutions across the EU and partner countries; this could bring project funding, enable knowledge-transfer from more CS-ready countries to the WB, and facilitate cooperation across different sectors.

Similarly, the NATO Smart Defence programmes can facilitate cross-sectoral cooperation in the field of cyber defence, since both Member States and partners are eligible on equal footing. This could enable WB countries to share the costs of developing advanced capabilities together. In addition, the NATO SPS programme allows Member States such as Croatia and Albania to connect to other countries in the WB and to benefit from training workshops and funding. Many programmes can involve non-government beneficiaries as well, but there is a lack of awareness about this among other sectors.

Regional cooperation in CS/IS among the countries of the SEE, as well as in the Western Balkans, is under-developed, non-systemic and primarily ad-hoc in character, with initiatives that have no clear direction and which are poised to die down with personnel changes and drying out of project funds. When it does happen, the regional CS cooperation mostly occurs between experts and professionals from specific areas (law enforcement, heads of technical departments within ministries or interested private sector parties). The asymmetric progression of CS legislature within the SEE states and the lack of resources, make this region rather unwelcome by the IT based economy.

The majority of regional institutions and initiatives tackle CS issues alongside their more pressing objectives: economic growth, public administration development, protection of personal or classified data, or the development of digital society. More tangible CS cooperation can be seen in cross-border police cooperation, while the military sector cooperation is still in the phase of acknowledging cyber threats and with activities focused on basic exchange of experience.

By analysing the goals and the activities of all processed regional initiatives in the last five years, the potential cooperation can roughly be put into four thematic groups. These groups can be used to outline the prime motivators within national and regional institutions for further regional cooperation:

- Cybercrime
- Economic/Administration Development and Protection of communication and information systems (CIS)
- Cyber Resilience
- Policy/EU integration Steering (Overarching)

With regards to cybercrime cooperation, although the region is still not attractive enough for high-end cybercrime threats, there are cybercrime dimensions that are a priority for all the SEE law enforcement actors, such as financial frauds or online child abuse. With organisations such as the SELEC and the SEEPAG, there is a basis for significant development of cooperation in these dimensions of cybercrime. This cooperation could be initiated via contacts with the national law enforcement professionals and heads of relevant departments, or national MPs working within the SEECP PA, or even through the RCC Secretariat by focusing on objectives within the "Justice" dimension of the SEE 2020 Strategy.

With regards to the economic/administration development and protection of the CIS, regional cooperation on CS can also be addressed as secondary objectives of other "non-security" priorities set by the RCC and EU integration processes, or objectives of other regional organisations such as the ReSPA. Implementing and harmonising information security standards in the region could be justified by other regional goals such as: economic growth, development of modern public administration, development of digital society, protection of the economy and critical infrastructure. It is important to communicate the importance of the impact CS/IS has on achieving these goals, and use existing frameworks (such as the RCC, the CEI or even the SEE PPP) to regionally gather stakeholders from the public, private and civil sector in concrete projects. This cooperation could be initiated via influencing the RCC agenda in the next three years or through civil initiatives supported by relevant regionally present international organisations.

With regards to cyber-resilience, quality of legislation, development of knowledge and the CS action potential of the Western Balkan states mainly depends on the input of their CS experts and on how well they are informed about new trends in CS. Organisations and initiatives like RACVIAC or SEENSA can be used to engage CS professionals from law enforcement and security–intelligence agencies, military, CERT structures, civil and private sectors, in trainings, joint projects, exchange of information and knowledge, to develop common standards, regulations and skills for building national and regional cyber resilience. For now the cooperation in this field is rather fragmented by professions, which sometimes leaves the impression of overlapping efforts.

With regards to policy/EU integration steering, the SEE Cooperation Process is surely the most influential regional initiative, gathering the heads of state and ministers of member states. Although perhaps hardest to influence, the SEECP could give the necessary push and legitimacy for developing a systemic regional CS cooperation. The Central European Initiative also gathers the highest state representatives through its Governmental Dimension, but the CEI can use its Network of Focal Points, or Parliamentary and Business Dimensions and its access to EU project funds to achieve regional CS cooperation through pursuing EU Digital Agenda goals within the SEE.

Bearing in mind that the existing initiatives and actors are in a very fragmented state, there is a pressing need for a systematic and authoritative coordination body (formal or informal), that would streamline further progress in cybersecurity among the WB states.

The Western Balkans countries have substantial guidance by the EU, the CoE, NATO, the ITU and other institutions on the ways to develop their national strategic, legal and operational environment. Besides, those and other international organisations, including the UNDP and the OSCE, provide a number of funding and support opportunities, despite the lack of strategic approach to support and a lack of general harmonisation of activities among those players. While on a formal level the countries in the region are progressing decently well with developing the necessary national

environments, there is an evident gap in implementation of the prescribed measures, utilisation of available international instruments for support, and regional cooperation through existing cooperation platforms for the SEE. This comes as a result of the missing political awareness, interest and strategic vision among the leaders and high-level decision-makers of the importance of cybersecurity; capacities among public institutions and policy-makers to comprehend the importance and complexity of the matter; the need for cooperation among countries as well as stakeholders; and capacities of other stakeholders to find meaningful ways to initiate national and regional projects and involve other sectors in broader cooperation.

8 Recommendations

Following the analysis of gaps in the performance of the WB countries, regional cooperation and the availability and applicability of IO support programmes, three sets of recommendations are provided:

1. for improving the state of play in the Western Balkan countries;
2. for a more systematic regional approach by international organisations;
3. for enhancing regional cooperation, both through the use of existing venues and the setting-up of a new light-format multistakeholder venue.

8.1 Recommendations for the Western Balkans countries

It is clear that more needs to be done in the Western Balkan countries in the development and implementation of regulatory frameworks on cybersecurity, and regarding cooperation with the relevant (non-state) stakeholders in the implementation and improvement of cybersecurity education. In particular, all countries need to:

- Enforce legislation and strategies;
- Establish the efficient and bureaucracy-free operational mechanisms for response to cyber-incidents, combating cybercrime, undertaking regular threat assessment and national situational awareness, etc.
- Raise the awareness of the political leadership and the creators of policy agenda
- Invest in the resources and capacities of the staff at Law Enforcement Agencies (LEA) and CERTs/CIRTs;
- Increase the capacities of all the stakeholders for cooperation across the sectors, especially involving those in charge of key infrastructure and services
- Promote PPP in the fields of protection of the economy and critical services, development of the cybersecurity industry and the establishment of comprehensive educational and competence building mechanisms to transform the labour market;
- Make substantial efforts to set in place sustainable educational programmes, build the capacity of users, develop excellence and expertise in cybersecurity research and protection, and increase the overall cybersecurity culture.

Each of the WB countriesshould be assisted in strengthening their internal capacities for cybersecurity.

- Political awareness and the strategic vision of the high-level decision makers in the WB about the political and socio-economic importance - risks but also potentials - of digital technologies, especially of cybersecurity, are at very low level. This causes a lack of effective developments in the CS/IS field. The EU integration process, international and regional platforms such as the OSCE, the CoE and NATO, as well as the existing SEE mechanisms such as the SEECP, can be used to raise this awareness.
- Institutional capacities for implementation of the CS/IS legislative frameworks in the WB are very limited. Since there is also lack of political will from the top to enforce substantial measures, policy-makers and implementing ministries are often satisfied with formalities, not seeing the overall complexity of cybersecurity policy. There is a strong need to enhance the policy and cooperation capacities of core public institutions - across different sectors,

from international relations, telecommunications and information society, security and economic growth to media, education, health and youth - to comprehend the relevance of cybersecurity for their field as well as the need for cooperation across the sectors and stakeholders in order to come up to efficient and robust policy solutions.

- National developments need to include stronger ties of public institutions with the private and non-government sectors, and facilitate public-private partnerships. A lack of understanding of the multidisciplinary and multistakeholder features of cybersecurity among policy-makers prevents cooperation across stakeholders. Besides, different professional cultures between diplomats and the public sector on the one hand and the private and civil sectors and academia on the other, increase possible misunderstandings and mistrust. Capacity building targeting diplomats, public services as well as key private sectors (especially the operators of critical infrastructure) and security sectors is needed to level the understanding of the matter, risks and best practices, while continuous joint exercises and simulations within each of the countries as well as across the region can enhance understanding and raise the readiness for operational cooperation.
- Many support programmes by international organisations also allow non-government beneficiaries to participate. The awareness about the overall political and policy cybersecurity environment and the work of and opportunities from IOs should be extended beyond institutions to other sectors, which are more agile and may galvanise national processes, initiate projects, bring various institutions in and stimulate cross-ministerial cooperation as well. Through the engagement of civil society and expert communities, countries would more likely use the available opportunities such as NATO programmes, the EU Horizon2020 and GEANT, and take part in the ITU/IMPACT, the ENISA, FIRST or Trusted Introducer (TF-CSIRT) activities. Stakeholders should also take advantage of the publicly available resources such as standards, support and expertise provided by international and regional organisations.

8.2 Recommendations for International Organisations

International organisations should also look for a more systematic, regional approach to cybersecurity in the Western Balkans. Such an approach can and should happen on several levels, which do not mutually exclude each other.

1. The IOs should use their existing bodies in the WB to foster cooperation and the exchange of knowledge in the WB.

   This option is relevant mostly for the EU and already mentioned ReSPA and the RCC. Both organisations are funded by the EU IPA funds and have some ICT-related issues. RCC can add to its existing bodies regular meetings of the designated national cybersecurity coordinators, whilst the ReSPA could create specific cybersecurity education programmes for regional state officials. A “Cybersecurity Academy” – an educational institution that would foster regional research and development efforts is necessary. Since none of the countries can create a meaningful, top-level institution of this kind on the regional level, with significant EU funding this would be an achievable goal.

2. The IOs should create new cybersecurity programmes and synergies for the region.

   The EU has only one programme (iPROCEEDS) that encompasses the whole of the Western Balkans. This practice should spill over to other cybersecurity issues than cybercrime.

Different cross-border programmes do not recognise cybersecurity as a topic of regional interest. Horizon 2020 and Multi-year IPA II programmes are an important opportunity for the countries of the Western Balkans, but the EU should be more proactive in this sense and provoke cooperation among the WB countries, by creating special regional funding for this purpose.

On the other hand, international organisations have good cooperation among themselves when it comes to cybersecurity. The EU and NATO closely cooperate on these issues, the OSCE's CBMs are taken into account by EU officials as a useful tool for fostering cooperation with Russia on cybersecurity etc. However, this does not mean the existence of a joint approach in CS. The nexus of such an approach exists with the two regional projects on cybercrime implemented by the CoE and funded through the EU IPA funds. This sort of cooperation should be fostered and nurtured. A joint approach is needed.

3. Country field offices of different IOs should work together on cybersecurity issues.

   Some field offices (the OSCE Missions to Serbia, Skopje, the UNDP Mission to Albania) have some smaller projects where different CS deficiencies are tackled on the national level. However, a regional approach would increase the outcomes of those projects and allow for better communication and knowledge exchange between similar institutions.

8.3 Recommendations for regional cooperation

Regional cooperation should be enhanced through a systematic, regional approach. The WB countries have scarce cooperation on these issues, mostly due to the fact that they are all still in the formative period, some of them still lacking the institutional and legal frameworks. One might argue that there are still no counterparts in each country to negotiate, discuss and cooperate. However, bilateral, regional and international cooperation is a reasonable way to achieve any progress for small nations.

8.3.1 Enhancing regional cooperation through existing institutions

The WB countries should foster cooperation, including through the existing regional institutions.

- Some countries in the region have more experience in assessing risks than others. It is therefore useful to enhance exchanges of information about incidents, knowledge and experiences with the policy and operational environment, and methodologies on risk assessment across the region. International venues such as ENISA, the ITU, the OSCE, the TF-CSIRT or FIRST should be better used in this regard, yet the existing regional venues such as the RACVIAC, that have proven the potential for discussions and exchange of experiences, can be explored, though more should be invested in involving other stakeholders in such venues.
- Close connectivity of the countries in the region means that there are common causes for many of the cyber-risks; besides, most of the critical infrastructure such as power grids is connected, and each security incident in one country could spill over to all other. It would be important for the countries of the region to agree on standards and procedures for mitigating risks and protecting critical information infrastructure and services together. ENISA and ITU resources could be used as guidance; such a thematic discussion could be incorporated into a multistakeholder discussion forum such as SEEDIG, in order to involve all the relevant actors; more advanced discussions could be

framed within the RACVIAC and even within the SEENSA Thematic Working Group for Cyber Defence; ultimately, a political agreement can be searched for within the SEECP, since it already has basic footprints of work in cybersecurity. Political readiness of at least one of the WB countries, however, is needed in order to push for such comprehensive process, as well as at least minimal support from the RCC.

- An exchange of the best practices on drafting and implementing regulations, especially at decision-making levels, might help policy makers overcome the inertia that prevents the many already drafted policy documents to be implemented, and that stops activities from being properly funded and supported. Experiences can be exchanged on developing and implementing cybersecurity strategies and action plans or in the development of educational programmes. Good experiences on setting up PPPs also need to be exchanged. While venues like the OSCE or even the RACVIAC might be used, integrating such experiences within the curriculum of the ReSPA for public servants might be a more sustainable and long-term approach.
- Given the few resources available for education, it might be advantageous to enhance academic exchanges and initiate collaborative educational programmes, especially on the academic and professional levels. The EU funding mechanisms could be used to support such initiatives.
- Given the transnational nature of cybercrime, the need for efficient cooperation of LEAs from the region in joint investigations is obvious. Since all LEAs still need to enhance their capacities, specific joint training activities might also be useful. Specific regional organisations like the SELEC and the SEEPAG with successful footprints in the field of police and judicial cooperation could be used as venues.
- Facilitating cooperation in the field of CS/IS within the SEE and even the CE institutions can boost the developments in countries of the Western Balkans as well. This is particularly important since some of the SEE and CE countries, that are not part of the WB, have advanced capacities and political awareness, as well as access to different EU or other support programmes. Besides, the CEI fund lines related to the EU Digital Agenda implementation, and in particular the pillar for strengthening online trust and security, could be used.
- There should be a comprehensive strategic effort for utilising the existing regional fora for cybersecurity cooperation and harmonising their activities in this field. The use of existing (even though rare) regional footprints such as the SEECP PA Report from 2015, the SEECP Bucharest Summit Declaration from 2014 or the SEENSA Thematic Working Group for Cyber Defence as the political leverage, could help boost further activities, while research on the most appropriate roles of each of the regional institutions vis-a-vis particular challenges, and a facilitated dialogue involving key actors present in each of the vital regional institutions, could help prepare a regional roadmap for cybersecurity, including the smart and coordinated use of the available international support mechanisms. In particular:
    - The SEECP has political leverage, and certain early footprints in cybersecurity that could be built on; it can be used as an agenda-setting mechanism, possibly through a particular push by the future chairs and the RCC as its operational institution;

- The RCC is the most active and operational regional institution that has political cooperation with almost all the other regional fora; even though in the forthcoming period it will likely focus on the economic development rather than on security, its' (at least light) support to cybersecurity initiatives could be placed under the RCC track for smart development;
- The RACVIAC is among the most active regional institutions in the field of CS/IS, with potentials for opening up its activities to a wider set of actors, and encouraging PPP;
- The ReSPA has a particular potential for capacity building among public institutions, yet it lacks expertise in digital issues and the CS/IS field, so support from foreign expert non-governmental organisations, educational institutions and the private sector would be needed; in addition, due to its light work on e-government and open government issues, the ReSPA has solid potential for multistakeholder projects and cooperation with other sectors;
- Specific "niche" organisations like the SELEC and the SEEPAG have proven successful in their activities with police and judicial cooperation, and they can play an important role in practical cooperation among the LEA in conducting investigations related to cybercrime;
- The SEEDIG is a unique forum for multistakeholder dialogue on Internet governance issues, and there is space for cybersecurity to feature strongly in the agenda; since both the agenda-setting and the discussions are open to all the stakeholders, this is a venue for strengthening the cross-sectoral dialogue and contacts, and initiating specific discussions.

Years 2016/2017 could be a favourable period for moving towards a more systemic regional cooperation within the CS field. In 2016, many of the regional initiatives face a new cycle of chairmanship, evaluation periods and the adoption of new strategic and action plans, which could be an opportunity for CS agenda setting.

8.3.2 Enhancing regional cooperation through the creation of a regional cybersecurity centre of excellence

Equally important, a particularly interesting option for strengthening regional cooperation would also be the creation of regional cybersecurity centre of excellence. Having a multidisciplinary feature of cybersecurity and cyberspace in general, and the necessity to approach cybersecurity challenges through a partnership between the security sector and different stakeholders, sectors and professions, an innovative approach to enhancing regional cooperation is a valid option for consideration.

The regional cybersecurity centre of excellence would work on several levels.

On a technical level, it would connect all regional CERTs/CSIRTs in a joint effort of sharing the information about incidents and defending regional computer networks from attacks. Since a number of the CS attacks are purely "regional" (meaning that hackers from one WB country attack websites of another WB country, or a specific type of attack, such as a bank fraud usually propagates from one country to the next), a regional proactive attitude would ultimately lead to better answers. Also, this would bridge the existing gap, since not all the countries have n-CERTs - or even if they

have one, most n-CERTs are under-equipped, under-staffed and incapable of dealing with sophisticated or massive CS attacks.

Apart from the operational level, a regional centre of excellence would entail policy-level units that would jointly work on the best institutional and legislative solutions in the region. It would serve as a platform for the exchange of best practices and lessons learned.

The centre would also offer tailor-made cybersecurity policy capacity building programs, as well as advanced technical training programmes. Since it would target various stakeholders, its alumni would enable the additional facilitation of community exchange and possible related policy-research activities. It could thus also embark on the pressing issues for all the WB countries – risk assessments and definition of critical infrastructure, with solutions to protect it.

The centre would be jointly funded by all the WB countries, but should also seek funding from the IOs present in the region as well as other donors, encompassing their CS portfolios in its training offerings. It would look to establish cooperation also with the existing regional institutions, primarily with the RCC, the RACVIAC and the ReSPA. The centre would initially draw expertise from renowned international and regional education, capacity building and research organisations, gradually building up its own sustainable base of regional experts.

Finally, the centre should initiate a regional form of public-private partnership and its first step would be the creation of a regional awareness raising campaign with the main international companies - gathering around a large scale campaign with a number of different activities which would serve to bridge the mental gap for cooperation on sensitive security issues between representatives of national institutions and the private sector (which already considers the whole region as one market); it would be the natural first step towards creating a sustainable and overarching PPP on the regional level.

The above-listed recommendations do not represent the exhaustive list of options. Specific follow-up discussion with the Swiss FDFA and other possible partners should be organised to identify the most rational, realistic and efficient follow-up to the current cybersecurity project conducted by DiploFoundation and the DCAF in the Western Balkans.

About the authors

Mr Adel Abusara, OSCE Mission to Serbia
Adel Abusara , is currently working on a project related to reforming the security sector in Serbia. Previously, Adel worked in the Serbian civil society sector on similar topics. He holds a BA in International Relations from the Faculty of Political Sciences, Belgrade University, and an MA in European Politics and Administration from the College of Europe in Bruges. Adel is passionate about a variety of cybersecurity related topics.

Ms ErandaBegaj, Institute for Democracy and Mediation, Albania
ErandaBegaj is a researcher in the field of cybersecurity for Western Balkan Countries. To this effect, she has contributed to many publications for different organisations working in the region, such as RACVIAC, ReSPA, DCAF, as well as DiploFoundation. Moreover she has worked in various positions in Albania's public administration, including at the National Agency on Information Society.

Mr Vladimir Erceg, Belgrade Centre for Security Policy, Serbia
Vladimir Erceg graduated from Faculty of Political Sciences in Belgrade, with a degree in International Relations. Erceg is a researcher and has published papers on integrity building in defence, national and regional cybersecurity policy, parliamentary oversight, emergency situations protection and rescue system, public procurement performance and anti-corruption measures in the security sector.

Ms Franziska Klopfer, the Geneva Centre for Democratic Control of Armed Forces (DCAF)
Franziska Klopfer is the Project Coordinator in the Operations Southeast Europe Division of DCAF, where she is currently leading the division’s civil society cooperation programme.

Ms Adriana Minović, Digital Watch, the Geneva Internet Platform
Adriana Minović is a lawyer with expertise in ICT industry. She was in charge of the harmonisation of Serbian legislation on electronic communication, information society and media, while working in the Ministry of ICT where she was also leading the process of chapter 10 of the acquis as part of the EU-accession negotiations. Apart from that, she is one of the associates of the first Serbian database about ICT regulation,'ICT law', and cooperates with Oxford and Columbia Universities as a legal expert on various projects. From 2016 she has been working with DiploFoundation as well as the Geneva Internet Platform, as one of the curators for the GIP Digital Watch and on various projects that are within her field of expertise.

Mr Vladimir Radunović, DiploFoundation (Diplo)
Vladimir Radunović is Director of e-diplomacy and cybersecurity educational and training programmes and a lecturer at Diplo. In addition, he is an expert on the Geneva Internet Platform, and serves as a member of the Advisory Board of the Global Forum on Cyber Expertise. He holds an MS in Electrical Engineering from the University of Belgrade and an MA in Contemporary Diplomacy from the University of Malta with a thesis on e-diplomacy, and has undertaken a PhD programme in cybersecurity. Vladimir was born and lives in Serbia.

Mr Predrag Tasevski, Founder of CyberSecurity.mk

Predrag Tasevski holds an MSc in Engineering in the field of Cybersecurity from Estonia, and a Post-Master degree in Security in Computer Systems and Communications from France. His research interests are in the field of cybersecurity, cyber-defence, security awareness, risk assessment, identity/risk management, cyber risk, cyber insurance, awareness-raising, socio-technical aspects, data science and hacktivism. Predrag is the author of two books, and has published at international conferences, in magazines and journals. He is a Macedonian representative of international NGOs and organisations. Today, he is an independent cybersecurity researcher, consultant and a founder of CyberSecurity.mk. Currently based in Frankfurt am Main, Germany.

About DiploFoundation

DiploFoundation is a leading global capacity development organisation in the field of Internet governance and digital policy.

Diplo was established by the governments of Switzerland and Malta with the goal of providing low cost, effective courses and training programmes in contemporary diplomacy and digital affairs, in particular for developing countries. Its main thematic focuses are on Internet governance (IG), e-diplomacy, e-participation, and cybersecurity.

Diplo's flagship publication 'An Introduction to Internet governance' is among the most widely used texts on IG, translated into all the UN languages and several more. Its online and in situ IG courses and training programmes have gathered more than 1500 alumni from 163 countries.

Diplo hosts the Geneva Internet Platform (GIP).

Diplo also provides customised courses and training both online and in situ, covering a wide range of subjectsincluding cybersecurity, Internet governance, data protection and e-diplomacy.

E-mail: ig@diplomacy.edu
Web: www.diplomacy.edu/cybersecurity