A NEW VIRTUAL BATTLEFIELD

How to prevent online radicalisation in the cyber security realm of the Western Balkans

RegionalCooperationCouncil

Financed by the European Union

Good.

Better.

Regional.

Title: A NEW VIRTUAL BATTLEFIELD - How to prevent online radicalisation in the cyber security realm of the Western Balkans

Publisher: Regional Cooperation Council
Trg Bosne i Hercegovine 1/V, 71000 Sarajevo
Bosnia and Herzegovina
Tel: +387 33 561 700; Fax: +387 33 561 701
E-mail: rcc@rcc.int
Website: www.rcc.int

Authors: Prof. Maura Conway
Sheelagh Brady

Editor: Amer Kapetanovic, RCC

Consulting editor: Zoran Popov, RCC

Design & Layout: Šejla Dizdarević

ISBN: 978-9926-402-11-2

December 2018

RegionalCooperationCouncil

A NEW VIRTUAL BATTLEFIELD - How to prevent online radicalisation in the cyber security realm

Sarajevo, December 2018.

TABLE OF CONTENTS

* This designation throughout this document is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence

Chapter 1

CYBER SECURITY IN THE WESTERN BALKANS

EXECUTIVE SUMMARY

The main objective of this study is to provide a comprehensive overview and analysis of the situation as regards cyber security in Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, Serbia and The Former Yugoslav Republic of Macedonia (hereafter WB6). Secondly, the study aims, ambitiously, to expand our understanding of cyber security beyond traditional narrow definitions to include information operations, with a focus in this study on the example of online radicalisation. To do this, the researchers have produced a two volume series. This report is Volume 1 of that series and focuses on traditional cyber security concerns.

In terms of approach, both desk based research and field consultations were conducted. A broad range of stakeholders were interviewed, from government, donor communities, the private sector, civil society and academia, to ensure breath of differing perspectives are represented.

A common condemnation of the WB6 in the past with regard to their cyber security posture has been that they do not have efficient institutional mechanisms, operational or legislative to adequately address this area. Reasons offered for this included a lack of political awareness and limited institutional capacity to recognise the risk. Such criticisms do not appear as valid today, and while the region is in no way immune from cyber security risks, the technology and economy gap between the region and Western Europe is said to be far shallower in the digital world than in the general economy. In fact, the pace of progress in this area in the WB6, while not ideal, is not totally at odds with that in many EU countries.

Similar to those EU countries too is that the WB6 conceive of cyber security narrowly and thus oftentimes limited to attacks that impact specific networks or devices. Yet, malicious attacks are only one variety of risk. Attacks on cognitive infrastructure, on people, society and systems of information and belief, often referred to as information operations or information based attacks are coming more to the fore, as malicious actors use online systems to exploit vulnerabilities in our information sphere. Volume 2 of this study examines extremism and online radicalisation in this light.

Findings and Recommendations

The driving force behind much of the WB6 activity in the area of cyber security is the European Union, by way of the Cyber Security Strategy of the European Union, NIS, and the Digital Agenda for Europe, amongst others. Indicative of the multi-layered approach the EU is taking in this area, the impetus for progress on cyber security also stems from the regional development agenda, such as the Multi-Annual Action Plan for a Regional Economic Area in the Western Balkans (MAP) and the Digital Agenda for the Western Balkans.

A variety of other documents and actors also play a role including the European Agenda on Security (2015), the Digital Single Market Strategy (2015); the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cyber Security Industry (2016); the Network and Information Security Directive; the EU General Data Protection Regulation (GDPR); the Directive 2013/40/EU on Attacks Against Information Systems; the Directive 2011/92/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography; the Framework Decision on Combating Fraud and Counterfeiting of Non-cash Means of Payment (2001); the Budapest Convention on Cybercrime (2001); the Digital Agenda for Europe (DAE); the European Union Agency for Network and Information Security (ENISA); the EU Computer Emergency Response Team (CSIRT-EU); Europol's Cybercrime Centre; NATO policy and action plan on cyber defence; CyberCrime@IPA and iProceeds; OSCE; International Telecommunication Union (ITU).

The WB6 have made and continue to make progress in harmonising their cyber security legislation and strategies in line with the EU framework. However, considerable deficits still remain in respect to implementation and operationalisation of practical responses. The most significant challenges are posed by (i) the lack of proper resourcing of Computer Security Incident Response Teams (CSIRTs); (ii) low levels of incident reporting; (iii) limited resourcing of bodies, such as CSIRTS, police, and prosecutors in respect of staffing, technology, and training, which is negatively impacting investigations and procedure; (iv) the lack of significant public-private partnerships, despite recognition of their value; (v) the lack of educational policies and programmes on Information and Communications Technology (ICT) and related areas within the WB6.

The following recommendations are provided to help address these challenges and to maximise progress in relation to the harmonisation of strategic and legal frameworks.

Recommendations

National-level recommendations

Despite progress in each of the WB6 with regard to cyber security, more needs to be done. The following recommendations should assist in achieving this.

- **Resource strategies and action plans** - A first step to concretely addressing this is to cost strategies and actions plans during the planning phase and then to reinforce such plans with dedicated funds. Solely relying on existing resources and/or donor funds will have significant negative impacts.
- **Create and/or improve cyber incident reporting structures** – One method to do this is to make it easier for citizens and businesses to report cyber security incidents. Many companies noted that they did not know how to report an incident, what information they would have to supply, and what and how much they could choose not to divulge. It is therefore recommended that CSIRTs reach out to such organisations and inform them about reporting processes and the nature and type of information that needs to be provided.
- **Raise awareness** - This could be addressed through a number of different measures, including through formal education and professional training. However, CSOs, community groups, and private sector providers should also be supported to provide information and knowledge in this area, to ensure a multi-layered approach.
- **Leverage existing expertise** - Creating networks of interested parties, such as the informal network initiated by OSCE and implemented by the Diplo Foundation and DCAF in Belgrade, or drawing on existing associations, such as those within the private sector, could be a very productive step. Furthermore, such networks of experts could assist in developing a more strategic approach to cyber security given their broad range of perspectives, experience, and vision.
- **Identify and develop Public-Private Partnerships (PPP) and build synergies** - Effective strategies in all policy realms are built on collaboration. Instead of just acknowledging the need for PPPs within cyber security (and CVE strategies; see Vol. 2), significant effort should be put into what such partnerships could look like and the areas that may most benefit from their establishment. Joint trainings are an obvious first step to building better relationships.
- **Review educational approach to ICT and Cyber Security** - The WB6 needs to undertake a comprehensive review of its educational approach to ICT and cyber security. This should not only enquire into what courses are required and at what levels, but include a longer term assessment of future needs in this area, and courses developed and offered based on this. It should almost certainly also include development of not just technology-based, but multi-disciplinary programmes to insure the competencies to support better strategic and operational implementation of cyber security strategy are available.

Regional-level recommendations

Many respondents agreed that progress in cyber security would benefit from a more joined-up and forward thinking regional approach, which would build on the work and structures of existing regional institutions, such as the RCC. This regional approach would make better use of scarce resources. Furthermore, it would illustrate a shared political will and proactive approach to cyber security. The following is therefore recommended:

- **Develop a more strategic approach to regional cooperation -** It is recommended that developing a strategic approach to cyber security should be done within existing frameworks, such as that of the EU, rather than creating new ones. For example, developing a WB6 regional cyber strategy, which identifies and sets out regional critical infrastructure, common minimum standards, a CIWIN, etc. This will help mitigate risk and ensure better overall CII protection.
- **Realign support of the international community to the strategy of the region -** The support of the international community is valued in this area, as in others, but does not come without criticisms. There is a need for greater discussion about what areas may benefit from international

support, what support would have the greatest impact, and related issues. Having a regional strategy would help identify headline issues and, in so doing, identify where best to direct such support. This may help to both alleviate criticisms about duplication of resources and streamline programmes into priority areas for the region.

- **Establish a regional centre of excellence -** A shared WB6 regional centre of excellence in cyber security would be of benefit. While this would not negate the need for basic, yet effective, minimum standards of equipment and technology at the economy level, more elaborate technology and equipment could be housed within a regional centre of excellence. This would reduce the cost to individual economies, yet provide them direct access to necessary high level technology, support, and expertise when needed.

ORGANISATIONS INTERVIEWED

Interviews were conducted with representatives from the following organisations. Their time, insights and opinions are greatly appreciated.

- Academy of Justice, Kosovo*
- American Chambers of Commerce, The Former Yugoslav Republic of Macedonia
- Balkan Investigative Reporting Network (BIRN)
- Belgrade Centre for Security Policy (BCSP), Serbia
- Bit Alliance, Bosnia and Herzegovina
- Boga & Associates, Law Firm, Albania
- Center for Democracy and Human Rights (CEDEM), Montenegro
- Center for Free Elections and Democracy (CESID), Serbia
- Center for Investigative Journalism SCOOP, The Former Yugoslav Republic of Macedonia
- Central Bank, Montenegro
- Centre for Security Studies, Bosnia and Herzegovina
- Cyber Security Specialist, The Former Yugoslav Republic of Macedonia
- DCAF, Serbia
- Diplo Foundation, Serbia
- European Movement in Albania
- General Directorate of State Police, Department of Economic Crime, Albania
- Institute for Democracy and Mediation (IDM), Albania
- IT Specialist, Albania
- IT Specialist, Bosnia and Herzegovina
- IT Specialist, Kosovo*
- Kosovo* Centre for Security Studies
- Kosovo* Forensics Agency
- Chamber of Information and Communication Technologies (MASIT) - ICT Chamber of Commerce, The Former Yugoslav Republic of Macedonia
- Melita Partners, Kosovo*
- Ministry of Defence, Bosnia and Herzegovina
- Ministry of Energy and Infrastructure, Albania
- Ministry of Internal Affairs, Montenegro
- Ministry of Security, Bosnia and Herzegovina
- CIRT, National Authority for Electronic Certification and Cyber Security, Albania
- National Computer Incident Response Team (CSIRT), The Former Yugoslav Republic of Macedonia
- NESECO, Bosnia and Herzegovina
- Organized Crime and Corruption Reporting Project (OCCRP)
- Organization for Security and Co-operation in Europe (OSCE) Albania
- OSCE, The Former Yugoslav Republic of Macedonia
- OSCE, Serbia
- Republic Agency for Electronic Communications and Postal Services, Serbia
- S&T, Montenegro
- Specialist on Radicalisation, The Former Yugoslav Republic of Macedonia
- State Prosecutors of Montenegro
- The Centre for Training in Judiciary and State Prosecution, Montenegro
- ICT Association, Kosovo*
- Tirana Prosecution Office, Albania
- Towersnet, Serbia
- University of Donja Gorica, Montenegro
- University of Pristina

LIST OF ABBREVIATIONS

AHT	Albania Hacker's Terrorist
ALCIRT	Albanian National Agency for Cyber Security
AKCESK	National Authority for Electronic Certification and Cyber Security
AKSHI	National Agency for Information Society
AMC	Albanian Muslim Community
AMRES	Academic Network of Serbia
BiH	Bosnia and Herzegovina
BSF	Belgrade Security Forum
CDCT	Committee on Counter Terrorism
CEAS	Centre for Euro-Atlantic Studies
CEF	Connecting Europe Facility
CII	Critical Information Infrastructure
CIP	Competitiveness and Innovation Programme
CIWIN	Critical Infrastructure Warning Information Network
CODEXTER	Committee of Experts on Terrorism
CSDP	Common Security and Defence Policy
CSIRT	Computer Emergency Response Team
CSO	Civil Society Organisation
CVE	Countering Violent Extremism
DAE	Digital Agenda for Europe
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DDoS	Distributed Denial-of-Service
DOS	Denial of Service
DSIs	Digital Service Infrastructures
EC	European Commission
ECI	European Critical Infrastructure
EC3	Europol's Cybercrime Centre
ECTC	Europol's European Counter Terrorism Centre
EKIP	Agency for Electronic Communications and Postal Services
ENISA	European Union Agency for Network and Information Security
ESI	European Structural and Investment
EU	European Union
EUIF	European Union Internet Forum
EUIRU	Europol's Internet Referral Unit
FP7	7th Framework Programme
GCA	Global Cybersecurity Agenda
GDPR	General Data Protection Regulation
GIFCT	Global Internet Forum to Counter Terrorism
HLCEG-R	High-Level Commission Expert Group on Radicalisation
H2020	Horizon 2020 Research and Innovation Framework Programme
IAP	International Association of Prosecutors
ICITAP	International Criminal Investigative Training Awareness Program
ICM	Islamic Community of Montenegro
ICT	Information and Communication Technology
IED	Improvised Explosive Devices
IISG	Integrative Internal Security Governance
IMPACT	International Multilateral Partnership against Cyber Threats
IOCTA	Internet Organised Crime Threat Assessment
IOM	International Organisation for Migration
IoT	Internet of Things
IP	Internet Protocols
IPA	Instrument for Pre-accession Assistance
IS	Islamic State
ISF	Internal Security Fund
ISP	Internet Service Providers
ITU	International Telecommunication Union
JHA	Justice Home Affairs
MAP REA	Multi-Annual Action Plan for a Regional Economic Area in the Western Balkans
MARnet	National Academic and Research Network
MIT	Massachusetts Institute of Technology
MOU	Memoranda of Understanding
NCCVECT	National Committee for Countering Violent Extremism and Countering Terrorism
NAEC	National Authority for Electronic Certification
NATO	North Atlantic Treaty Organization
NBS	National Bank of Serbia
NGO	Non-Governmental Organisations
NIS	Network and Information Security Directive
OTA	Operational Technical Agency
PCVE	Preventing and Countering Violent Extremism
POC	Point of Contact
PPP	Public-Private Partnership
RAN	Radicalisation Awareness Network
RATEL	Republic Agency for Electronic Communications and Postal Services
RCC	Regional Cooperation Council
R&D	Research and Development
RUSI	Royal United Service Institute
SIPA	State Investigation and Protection Agency
TDO	The Dark Lord
TSO	Transmission System Operators
UK	United Kingdom
UN	United Nations
UNCTC	United Nations Counter Terrorism Committee
UNCTED	United Nations Counterterrorism Executive Directorate
UNDP	United Nations Development Programme
UNODC	United Nations Office on Drugs and Crime
WBBSi	Western Balkan Border Security initiative
WBCSi	Western Balkan Counter Serious Crime initiative
WBCTi	Western Balkan Counter-Terrorism initiative.

1. INTRODUCTION

There were 3.8 billion internet users globally in 2017, an increase from 2 billion in 2015. That equates to approximately 51% of the world's population. It is predicted that the number of users will rise to 6 billion by 2022 and 7.6 billion by 2030, equating to approximately 90% of the world's population 6 years old and above. Coupled with increasing numbers of users is an increased volume of activity on the internet. For example, the first website was launched in 1991; today there are over 1.2 billion websites in existence.[1] In 2016 there were approximately 2.28 billion social media users worldwide; this is estimated to grow to 2.77 billion in 2019, and 3 billion by 2021.[2] In fact, Microsoft suggest that data volumes online will be 50 times greater in 2020 than they were in 2016. While Intel claims that, given 'big data' and the Internet of Things (IoT), the number of smart devices will have grown from 2 billion in 2006 to 200 billion by 2020.[3]

These statistics and projections are important, especially if Braithwaite's assertion as regards crime in the offline world holds for cybercrime too.[4] Braithwaite claimed that as the population increases so too does the crime rate (per capita). If the increase in internet users and targets has the same impact as population growth in the offline world, one would expect to see a significant and continuing increase in cyber attacks. Findings from the European Union Agency for Network and Information Security (ENISA) may be emerging evidence that this is already happening. In their 2017 review, ENISA noted that the "complexity of attacks and sophistication of malicious actions in cyberspace continue to increase".[5] The greater number of users—in this case, targets—is also likely to have an impact on the level, and probably also sophistication, of cyber influence operations, including by states, extremists, and terrorists, and a variety of other information entrepreneurs, such as online purveyors of so-called 'fake news'. ENISA (2017) noted that:

Monetization of cybercrime is becoming the main motive of threat agents, in particular cyber-criminals. They take advantage of anonymity offered by the use of digital currencies; State-sponsored actors are one of the most omnipresent malicious agents in cyberspace. They are a top concern of commercial and governmental defenders; Cyber-war is entering dynamically into cyberspace creating increased concerns to critical infrastructure operators, especially in areas that suffer some sort of cyber crises.[6]

It is important and timely therefore to question if our contemporary conceptions of cyber security, which largely focus on hard or kinetic attacks, such as cyber attacks and cybercrime, and omit online information operations, such as online radicalisation, hate speech and 'fake news', are fit for purpose.

1 Morgan, S. (2017). 'Cybercrime Damages $6 Trillion By 2021', Cybersecurity Ventures, 16 Oct.: *https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016*.

2 Statistica (2018). 'Number of Social Network Users Worldwide from 2010 to 2021 (in Billions)': *https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users*.

3 Morgan (2017). 'Cybercrime Damages $6 Trillion By 2021'.

4 Braithwaite, J. (1975) 'Population Growth and Crime', Australian and New Zealand Journal of Criminology, 8(1).

5 See ENISA (2018). ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends, Heraklion, Greece: ENISA: *https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017*.

6 ENISA (2018). ENISA Threat Landscape Report 2017, p.7.

Table 1. Growth in internet use in the WB6 between 2000 and 2017

	2000[a]	2017[b]
ALBANIA	.1%	66%
BOSNIA AND HERZEGOVINA	1.1%	81%
KOSOVO*	-----	80%
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA	2.5%	76%
MONTENEGRO	18.4%	70%
SERBIA	12.3%	72%

Sources: [a] Internet Live Stats (2018). 'Internet Users': *http://www.internetlivestats.com/internet-users/*; [b] Internet World Stats (2017). 'Europe': *https://www.internetworldstats.com/europa2.htm*.

1.1 Objective of the study

The WB6 witnessed significant growth in internet use between 2000 and 2017 (see Table 1). The main objective of this study is to provide a comprehensive overview and analysis of the situation as regards cyber security in Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, Serbia, and The Former Yugoslav Republic of Macedonia (hereafter WB6). Table 2 provides a synopsis of relevant information and findings in respect to each of the WB6 and Cyber Security. The aim, in part, of this is to assess how the WB6 compare in respect to the European Union's activities in this area. This is timely, given the European Commission's (EC) launch of the Digital Agenda for the Western Balkans in June 2018, which aims to "support the transition of the region into a digital economy and bring the benefits of the digital transformation, such as faster economic growth, more jobs, and better services"[7], by focusing on areas such as (i) lowering roaming charges (ii) connectivity (iii) cyber security, trust and digitalisation of industry (iv) digital economy and society, and (v) research and innovation. Having an effective cyber security framework is also imperative for achieving the commitments made by WB6 leaders in 2017's Multi-Annual Action Plan on Regional Economic Area (MAP REA).[8]

At the same time, this study also aims, ambitiously, to expand our understanding of cyber security to encompass not just cyber attacks and cybercrime, but also cyber influence operations. These 'hard' (i.e. cyber attacks, including cybercrime) and 'soft' (i.e. 'fake news', online radicalisation, etc.) aspects of malicious cyber activity are often treated separately from each other, with attention to 'hard' issues privileged over 'soft'. The genesis of our combined approach stems from a growing awareness by the Regional Cooperation Council (RCC) that the role of the internet in information operations cannot and should not be viewed in isolation from other areas of cyber security. The realm of cyber influence operations is murky, difficult to research and only recently receiving sustained attention from researchers, policymakers, media, and others. It is impossible to adequately treat all of its various aspects in a study of this nature. The focus in this study is therefore on a single key example of contemporary influence operations: online radicalisation, where the internet is leveraged to gain sympathy and attract supporters for a variety of extremist and terrorist causes. This stems from an understanding that on-

7 European Commission (2018). 'European Commission Launches Digital Agenda for the Western Balkans', Press Release, 25 June: *http://europa.eu/rapid/press-release_IP-18-4242_en.htm*.

8 See RCC (2018). 'Multi-Annual Action Plan for a Regional Economic Area in the Western Balkans': *https://www.rcc.int/priority_areas/39/multi-annual-action-plan-for-a-regional-economic-area-in-the-western-balkans--map*.

line terrorist activity has to-date focused less on conducting cyber terrorism and more on leveraging cyber spaces and tools for other purposes, including radicalisation, recruitment, attack planning, and similar. Such an understanding on the part of the RCC has motivated them to commission this study in order to identify the linkages and overlaps between traditional narrow understandings of cyber security and a new and more expansive approach that takes 'soft' cyber security issues, such as online radicalisation, seriously. This bridging of the existing conceptual gap will, the RCC believes, assist them in implementation of their commitments in the cyber security domain, including their responsibilities in preventing and countering (online) violent extremism and terrorism.

To do this, the study is divided into two volumes; this is the first volume. It is divided into five sections. The first section discusses the relevant literatures, including definitional choices, and supplies a brief rundown of our methodology. The second section identifies EU legislative instruments, policies, and organisations that have influenced the WB6's cyber security posture. Section three treats cyber security in the WB6 as traditionally or narrowly defined, so having an emphasis on cyber attacks, cybercrime, and related issues. Section four is composed of mini-cases studies of all WB6 economies, presenting the main actors responsible for cyber security in each economy, their keys activities, and existing challenges in this area. Volume two applies a similar structure as it pertains to violent online extremism, the terrorism-internet nexus, and online radicalisation from the WB6 perspective. Each report ends with conclusions and recommendations.

	ALBANIA	BOSNIA AND HERZEGOVINA	KOSOVO*	THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA	MONTENEGRO	SERBIA
Budapest Convention on Cybercrime	Ratified 2002 24/7 Point of Contact (POC)	Ratified 2006 24/7 POC	24/7 POC	Ratified 2004 24/7 POC	Ratified 2010 24/7 POC	Ratified 2009 24/7 POC
National CIRT	✓ 2016	Very limited functionality 2017	✓ 2016	✓ 2016	✓ 2012	✓ 2016
CIRT Location	National Authority of Electronic Certification and Cyber Security	Ministry of Security	Regulatory Authority for Electronic and Postal Communications	Agency for Electronic Communications	Ministry of Public Administration	Republic Agency for Electronic Communications and Postal Services
Law on Cyber Security	✓ Adopted 2017	×	✓ Adopted 2010	×	✓ Adopted 2010	✓ Adopted 2016
Cyber Security Strategy	Policy acts in lieu, 2015-2017	×	Strategy and action plan 2016	Strategy Adopted in July 2018	Strategy and action plan 2018-2021 (2nd strat.)	✓ no action plan 2017
3rd level education on Information Security	×	✓	✓	✓	✓ multi-disciplinary	×
Critical Information Infrastructure Defined	✓	×	✓	×		×
CVE/Terrorism Strategy includes reference to cyber/ online	✓	✓	✓	✓	✓	✓
Key Challenges	Technical, financial, expertise and accessing and retention staffing					

Table 2. Synopsis of relevant information and findings in respect to each of the WB6 and Cyber Security

1.2 Cyber Security

Cyber security[9] is often described as the process of protecting online systems, networks, information/data and programmes from digital attack. More specifically, the EU defines it as:

[T]he safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber Security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained within.[10]

Adopted in this study however is Von Solms and Van Niekerk's (2012) much wider definition of cyber security as:

[T]he protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace.[11]

This definition illustrates how cyber security is far more complex than just its information and/or ICT security components. It includes, in addition, the security and even wellbeing of users and the security and protection of their assets that can be accessed or reached via cyberspace. Cyber security, on this definition, stretches from protection of critical infrastructures be it international, regional, national, or local, such as the electric power grid and air traffic control systems to the security of individual internet users – such as via limiting their exposure to online bullying; cybercrime, including online fraud and extortion; or online radicalisation – but while also protecting those same users' digital rights and freedoms. In terms of threat actors, hostile states, terrorists, criminals, and other malicious individuals and groups are aware that increased global digitalisation provides opportunities to them worth maximising. Targets are also many and varied. Particular threats are posed by attacks on critical infrastructure, but are not restricted to these, and can include informational attacks on elections, social cohesion, and the like.

The European Union defines Critical Infrastructure as an:

[A]n asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.[12]

Such critical infrastructures are often highly interconnected and mutually dependent, both physically and technologically. Therefore, when one is targeted it can have serious repercussions for others too. The scale and scope of this can vary from being quite localised to reaching far beyond domestic or regional borders.[13] In addition to defining critical infrastructure generally, Directive 2008/114/EC of the Council of the European Union also defined 'European Critical Infrastructure (ECI)' as:

[C]ritical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependence on other types of infrastructure. [14]

In light of the Digital Agenda for the Western Balkans, the EU's digital single market strategy,[15] and the World Bank's Balkans Digital Highway Initiative[16], it is pertinent for the WB6 to follow suit and set out and define what could be considered regional critical infrastructure. For example, a shared regional utility infrastructure could significantly benefit the region, both from a user and economic perspective. Bosnia and Herzegovina and Serbia have yet to formally define CII in their legislation or strategies, but the remainder of the WB6 have definitions included in their cyber security strategies.

A sub-category of critical infrastructure is Critical Information Infrastructure (CII), defined as "ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.)".[17] Governments therefore have a key role in ensuring the security of cyberspace, similar to their responsibilities for critical physical infrastructure in the offline world. However, to do this, cooperation between countries, both at regional and international levels, is required. An example of this at the European level is the Critical Infrastructure Warning Information Network (CIWIN). The CIWIN, which has been running since 2013, was developed as:

[A] Commission owned protected public internet based information and communication system, offering recognised members of the EU's CIP community the opportunity to exchange and discuss CIP-related information, studies and/or good practices across all EU Member States and in all relevant sectors of economic activity.[18]

The WB6 may benefit from a similar network. Dialogue and cooperation with the private sector and civil society is critical to ensuring both policy and operational success given the interconnectivity of critical infrastructures, technology, and users, especially because a large proportion of CI is owned by private companies, such as telecommunications service operators, banks, and transmission system operators (TSOs). They too have responsibility in the area of cyber security. Worth noting, further, is that cyber security does not only relate to protection against man made attacks, but includes protection of ICT infrastructure from all threats and risks, such as those stemming from natural disasters and unforeseen circumstances.

That said, not all, or even most, cyber attacks target critical infrastructure. Instead of being matters of national security, many breaches of cyber security are of a more routine criminal nature, except having a significant online component. Many such incidents fall into the category of cybercrime. Cybercrime is described in Europol's Internet Organised Crime Threat Assessment (IOCTA) "as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In essence, without the internet these crimes could not be committed".[19] These include online scams, malware, ransomware, email bombing, virus dissemination, logic bombs, electronic money laundering, sales and investment fraud, eavesdropping and surveillance, hacking, cyber stalking, cyber bullying, identity theft, and child soliciting and abuse.

It has been difficult to obtain verified statistics and information on cyber attacks and cybercrimes in the WB6. Those that are available are generally not directly comparable as they do not only always include the same types of crime. This is evident in the difference in the number of incidents reported in Table 3, which shows those statistics that are available. This lack of statistics is interesting in itself as it illustrates that the WB6's CSIRTs are not yet functioning at a level that facilitates reliable monitoring, recording, and reporting. The lack of statistics should not be seen as the absence of attacks nor solely the fault of CSIRTs, however. There is a high degree of underreporting of cyber attacks globally not just in the WB6, which makes gathering reliable statistics difficult. Furthermore, organisations, both private and public, are often unaware that they have been the victim of attack and thus have nothing to report. Given the lack of statistics and in an effort to highlight the type, scale, and scope of incidents in the region, Table 4 illustrates a selection of cyber incidents discussed in WB6 media between 2013 and 2018.

9 There are a very large number of definitions of cyber security available in policy documents, the academic literature, etc. It is not within the remit of this report to argue the merits or demerits of these various approaches, which would require a whole study in itself.

10 European Commission (2013). *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels: High Representative of the European Union for Foreign Affairs and Security Policy, p. 3: *http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf*.

11 Von Solms, R. and Van Niekerk, J. (2012). 'From Information Security to Cyber Security', Computers & Security, Vol. 39, p.101.

12 Council Directive 2008/114/EC (2008) on The Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, 8 Dec., p. 3: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN*.

13 Rinaldi, S.M., Peerenboom, J.P., and Kelly, T.K. (2001). 'Identifying, Understanding, and Analysing Critical Infrastructure Interdependencies', IEEE Control Systems, 21(6).

14 Council Directive 2008/114/EC (2008) on The Identification and Designation of European Critical Infrastructures, p.77.

15 "The Digital Single Market denotes the strategy of the European Commission to ensure access to online activities for individuals and businesses under conditions of fair competition, consumer and data protection, removing geo-blocking and copyright issues". See European Commission (2018), 'Shaping the Digital Single Market': *https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market*.

16 "The World Bank Balkans Digital Highway Initiative is a new study that will investigate whether it is possible to improve the regional interconnectivity in the Western Balkans and increase access to the Internet for people by establishing a regional broadband internet infrastructure over transmission grids of state-owned energy companies. The initiative may pave the way for the first joint collaboration on digital connectivity among Albania, Bosnia and Herzegovina, The Former Yugoslav Republic of Macedonia, Kosovo,* Montenegro, and Serbia, if the assumptions on the significance of optical fiber assets owned by the operators of transmission systems are justified from an economic, technical, and regulatory point of view." See World Bank (2017). 'Brief: Balkans Digital Highway Initiative', 9 May: *http://www.worldbank.org/en/country/kosovo/brief/balkans-digital-highway-initiative*.

17 European Commission (2005). 'Green Paper: European Programme for Critical Infrastructure Protection', 17 Nov., p. 19: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=BG*.

18 For more information, see the Critical Infrastructure Warning Information Network's (CIWIN) webpage at *https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en*.

19 Europol (2017). Internet Organised Crime Threat Assessment 2017 (IOCTA 2017), The Hague: Europol, p.18: *https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf*.

Table 3. Reported Cyber Security Incidents 2017	
ALBANIA	NA
BOSNIA AND HERZEGOVINA	NA
KOSOVO*	NA
MONTENEGRO	385[a]
SERBIA	20[b] 22
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA	72[c] 23

Sources: [a] Government of Montenegro (2017). *Cybersecurity Strategy of Montenegro, 2018 - 2021*, Podgorica: Ministry of Public Administration, p. 20: *http://www.mju.gov.me/ResourceManager/FileDownload.aspx?rid=305198&rType=2&file=-Cyber%20Security%20Strategy%20of%20Montenegro%202018-2021%20eng.pdf*; [b] Statistical Office of the Republic of Serbia Statistical Release SK12, Number 193 • Year LXVIII, 16.07.2018, Judiciary statistics, p. 6: *http://publikacije.stat.gov.rs/G2018/PdfE/G20181193.pdf*; [c] 'Macedonia 2018 Crime & Safety Report': *https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=23844*.

In 2017, Europol reported that the most common attacks utilised a particular type of malware known as ransomware.[22] Ransomware is a type of malicious software or 'malware' that upon infecting a system locks or encrypts victims' data and threatens to permanently block access to it unless a ransom is paid. The May 2017 WannaCry and June 2017 Petya/NotPetya ransomware attacks impacted globally; lower-level ransomware attacks on small firms and individuals are increasingly commonplace however, as are the use of other types of malware, including banking Trojans, and a wide variety of phishing scams. It's worth noting here that it is often difficult, due to the similar tools and techniques used, to attribute cyber attacks to particular actors (e.g. financially motivated cybercriminals versus a hostile state or its proxies), the motives for attacks – especially national or global-level attacks – are thus often a matter for debate and/or remain obscure. McAfee, announcing their June 2018 *Labs Threat Report*, reported a 31% decline in new malware, but noting that threat actors were evolving their technologies to do things better.[23]

1.3 Information Operations

As the preceding discussion illustrates, when policymakers, media, and publics discuss cyber security they generally think about attacks that impact specific networks or devices. Malicious cyber attacks are only one variety of cyber risk however. Information operations or information-based 'attacks', on the other hand, focus on "cognitive infrastructure, on people themselves, on society, and on systems of information and belief".[24] The power of strategies of disinformation and misinformation to manipulate is coming more to the fore, especially in the context of so-called 'fake news'. Algorithms, clickbait, advertising, and social media give fake news producers access to data and analytics on content performance and visitor demographics, which are very powerful commodities. These are being used to exploit vulnerabilities in our information systems. A wide variety of malicious actors, from states with traditional geopolitical interests to financially-motivated information entrepreneurs, are today weaponising the Internet, particularly social media, to forward their goals.

Take, for example, the town of Veles in The Former Yugoslav Republic of Macedonia. It came to prominence in 2016, just before the US Presidential Election. Young people from the town were alleged to have made considerable sums of money flooding the internet with viral content, much of which was untrue, supporting Donald Trump.[25] Researchers from the Massachusetts Institute of Technology (MIT) found that false information is 70% more likely to be retweeted than fact, and that false stories reach 1,500 people six times quicker on average than a true story does, outperforming on every subject – including terrorism and war.[26] Investigations are still continuing, but it is interesting to reflect that it remains unclear that anyone involved in the Veles online operation actually broke the law. Nonetheless, these WB6-based information 'entrepreneurs' illustrate how together the power of social media, digital advertising revenue, and political partisanship can produce a toxic brew.[27]

In terms of online information operations and the (cyber) security risks posed by these, fake news is an emerging area of policy concern and academic research. We know considerably more, however, about violent extremists and terrorists who have, for some time, been utilising the internet to "communicate, collaborate and convince" and it is their activities that will be concentrated on in this study.[28] Treatment of terrorist use of the internet as a cyber security issue may seem unremarkable, excepting that it's not so-called 'cyberterrorism' that is focused on herein. Terrorism and the internet intersect in two main ways. NATO's *Tallinn Manual* describes 'cyber terror' as "[c]yber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population".[29] The cyberterrorism threat is often portrayed via worst case scenarios, from using cyber means to shut down the electric power grid to contaminating a major water supply.[30] Everyday terrorist use of the Internet, including for publicity, radicalisation, recruitment, financing, coordination, attack-planning, and a variety of other purposes, is much more commonplace however. This differentiation between cyberterrorism and terrorist use of the internet[31] is important in the context of this study for two reasons. First, the distinction goes to the heart of the issue as regards traditional narrow conceptions of cyber security, which focus on the cyberterrorism threat, while ignoring what has thus far turned out to be the greater threat: everyday terrorist use of the internet. Second, there is no evidence to suggest that an incident of cyberterrorism has occurred or is imminently likely in any of the WB6, but there is ample evidence of extremist and terrorist internet use, which will be discussed in more detail in Volume 2.

1.4 Methodology

This research employed a mixed methods approach, which allowed for the combination of data from a variety of different sources. The process was broken down into three phases: (i) desk-based research, (ii) field assessment and consultation, and (iii) report writing. Given that the topics under review (i.e. cyber security as traditionally conceived and information operations, with a particular focus on extremism, terrorism and online radicalisation) are generally viewed as distinct, our initial approach to the desk-based research was two-pronged: we undertook a separate literature review and document analysis in respect of each of cyber security and online radicalisation. Each was then examined to identify linkages and overlaps between them. All relevant issues were then followed-up in the field research in the WB6.

All interviews, excepting four conducted via Skype, were carried out in the WB6 in May and June 2018. Forty-five interviews were conducted in total; all were semi-structured in nature. Of these, nine were conducted in respect to Albania, eight in Bosnia and Herzegovina, seven in Kosovo*, seven in Montenegro, seven in The Former Yugoslav Republic of Macedonia, and seven in Serbia. To ensure inclusion of a wide breath of perspectives, stakeholders from five key fields were initially targeted: government, donor communities, the private sector, civil society, and academia. A thematic guide, based on the literature reviews, was developed for the interviews to ensure consistency across them. A combination of thematic and content analysis was then conducted. This allowed for flexibility, whilst still producing rich, detailed, and complex description of the data. A similar thematic interview model was used during all interviews. The interviews were not electronically recorded, but detailed notes were taken throughout. All interviewees were provided with a unique code to ensure anonymity, codes ranged from RB1 to RB45.

Given the scale and scope of this project, a snow-balling method of sampling was used when decid-

20 Criminal offences against safety of computer data, consisting of damaging computer data and programmes (4); computer sabotage (1); computer fraud (11); unauthorised access to secured computer, computer network and electronic data processing (3); unauthorised use of computers or computer network (1). In Statistical Office of the Republic of Serbia Statistical Release SK12, Number 193 • Year LXVIII, 16.07.2018, Judiciary statistics, p. 6: *http://publikacije.stat.gov.rs/G2018/PdfE/G20181193.pdf*

21 In 2017, there were 72 documented cybercrime offenses in The Former Yugoslav Republic of Macedonia, with damage and illegal access to computer systems being the most common, followed by computer fraud. See US Department of State, Bureau of Diplomatic Security (2018). 'Macedonia 2018 Crime & Safety Report': *https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=23844*

22 Europol (2017). *IOCTA 2017*, p.10.

23 Beek, C., Dunton, T., Grobman, S., Karlton, M., Minihane, N., Palm, C., Peterson, E., Samani, R., Schmugar, C., Sims, R., Sommer, D., and Sun, B. (2018). McAfee Labs Threats Report, June, Santa Clara, CA.: McAfee: *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf*.

24 Morgan, J. and DiResta, R. (2018). 'Information Operations are a Cybersecurity Problem: Toward a New Strategic Paradigm to Combat Disinformation', Just Security, 10 July: *https://www.justsecurity.org/59152/information-operations-cybersecurity-problem-strategic-paradigm-combat-disinformation*.

25 Subramanian, S. (2017). 'Inside the Macedonian Fake-news Complex', Wired, 15 Feb.: *https://www.wired.com/2017/02/veles-macedonia-fake-news/*.

26 Vosoughi, S., Roy, D., and Aral, S. (2018). 'The Spread of True and False News Online', Science, 359(6380). See also Meyer, R. (2018). 'The Grim Conclusions of the Largest-Ever Study of Fake News', The Atlantic, 8 March: *https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/*.

27 Kirby, E.J. (2016). 'The City Getting Rich from Fake News', BBC News, 5 Dec.: *https://www.bbc.com/news/magazine-38168281*.

28 Von Behr, I., Reding, A., Edwards, C., and Gribbon, L. (2013). Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism, Brussels: RAND Europe, p. 3 and p.31: *https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf*.

29 NATO Cooperative Cyber Defense Centre of Excellence (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, UK: Cambridge University Press, p.104.

30 Conway, M. (2017). 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research,' *Studies in Conflict & Terrorism*, 40(1), pp.'s 77-98.

31 Conway, M. (2017). 'Determining the Role of the Internet in Violent Extremism and Terrorism', pp.'s 77-98.

ing who to interview. Unlike traditional snowball sampling, where individuals interviewed nominate potential other respondents, a less traditional approach was used. If respondents raised an issue or identified an organisation that it was felt by the interviewer might be of relevance, that organisation or a similar organisation professionally tasked around the issue was contacted. For example, prosecutors interviewed highlighted gaps in training, so representatives from organisations that provide training to prosecutors and judges were later interviewed. This allowed for a broadened range of respondents to be included in the study, resulting in a more multi-disciplinary perspective.

Table 4. A selection of reported cyber attacks in WB6 between 2013 and 2018[34]

ALBANIA	2014	The group called Redanons_al attacked and defaced the web pages of the interior and foreign ministries and those of the ministries of integration, agriculture, energy, welfare, innovation and technology, health and urban development.[a]
	2016	The self-proclaimed Albania Hacker's Terrorist (AHT) crew attacked a website and posted a message against the Greek JP-AVAX construction company. The message had mainly nationalist content.[b]
	2017	Anonymous Albania increased its cyber attacks on the Albanian government. One example, related to an attack on the website of EcoTirana[c35] in response to the destruction of the Bus Station Park by Tirana mayor Erion Veliaj.[d]
BOSNIA AND HERZEGOVINA	2016	Bosnian authorities arrested two suspected members of DD4BC, a cybercrime group based in Republika Srpska (RS), who were allegedly involved in Denial of Service type attacks, demanding Bitcoin payments to return services.[e]
KOSOVO*	2012	A massive amount of data from the official US National Weather Service website was leaked online over a number of days by "Kosovo* Hacker's Security",[f] an Albanian hacktivist group from Kosovo*.
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA	2017	Reports claimed that Rxr, a hacker, penetrated some of The Former Yugoslav Republic of Macedonia's government institutions. It was reported that no obvious threats or warnings were contained in the defacement message.
MONTENEGRO	2017	A Russian cyber-espionage group, Fancy Bear, was alleged to have conducted a number of attacks again Montenegrin institutions. The Defence Ministry is said to have been targeted. These attacks predominately related to 'phishing emails', which if opened were said to have installed the Game Fish malware on the victim's system[g]
SERBIA	2013	The Tesla Team, a Serbian hacker group, targeted government websites belonging to various economies. For example, the Albanian Ministry of Economy, Trade, and Energy (mete.gov.al), the Albanian Ministry of Finance, Court of Bosnia and Herzegovina (sudbih.gov.ba), and Ghana's Ministry of Economic Planning (mofep.gov.gh). The hackers did not deface any of the websites.[h]
	2014	The Pescanik.net website, amongst others, was brought down by a Denial of Service (DoS) attack[i], directly after publishing allegations that Serbian Interior Minister Nebojsa Stefanovic had plagiarised parts of his PhD thesis.
	2017	An electronic fraud attack was targeted at the National Bank of Serbia (NBS). The NBS was requested to make a payment of holographic foil into an account into a Polish bank. Holographic foil is used for the preparation of specific hologram protection on banknotes, identity cards, passports and similar documents.[j]
	2018	WebStresser.org, the world's largest online attack-for-hire service, behind at least four million cyber attacks in the past three years, was shut down by a coordinated international police operation. It had an extraordinary 136,000 registered users when it was taken offline, and had been responsible since 2015 for distributed denial-of-service (DDoS) attacks on governments, police services, banks, and businesses of all sizes – causing chaos and frequently huge financial losses. The website was believed to have been set up and run by a 19-year-old Serbian hacker who goes by the nickname "mirk".[k]
	2018	Serbian authorities arrested a man on suspicion of being associated with "The Dark Overlord" (TDO), a prolific hacker or hacking collective that had a number of breaches and cyber-extortion campaigns to its name in the previous two year.[l]

Sources:[a] Likmeta, B. (2014). 'Hackers Deface Albania Ministerial Websites', BalkanInsight, 29 July: *http://www.balkaninsight.com/en/article/hackers-deface-ALBANIA-government-websites*; [b] Aspida Cyber Security (2016). 'Albanian Hackers Attack JP-Avax!', 7 Nov.: *https://cyber.aspida.org/ALBANIAn-hackers-attack-jp-avax/*; [c] See *http://www.ecotirana.com*; [d] Tomovic, D. and Zivanovic, M. (2018). 'Russia's Fancy Bear Hacks its Way Into Montenegro', BalkanInsight, 5 March: *http://www.balkaninsight.com/en/article/russia-s-fancy-bear-hacks-its-way-into-montenegro-03-01-2018*; [e] E Hacking News (2013). 'Government Websites Hacked, Database Leaked by TeslaTeam', 5 Dec.: *http://www.ehackingnews.com/2013/12/government-websites-hacked-database.html*; [f] Danas, T. (2014). 'Peščanik Website "Came Under DDoS Attack"', b92, 4 June: *https://www.b92.net/eng/news/crimes.php?yyyy=2014&mm=06&dd=04&nav_id=90561*; [g] The Telegraf (2017). 'There Was a Big Cyber-attack on the National Bank of Serbia: 175,500 Euros Stolen!', 24 May: *http://www.telegraf.rs/english/2793841-there-was-a-big-cyber-attack-on-the-national-bank-of-serbia-175500-euros-stolen*; [h] Cluskey, P. (2018). 'WebStresser.org Site Linked to Global Cyberattacks is Shut Down', Irish Times, 30 April: *https://www.irishtimes.com/news/world/europe/webstresser-org-site-linked-to-global-cyberattacks-is-shut-down-1.3478112*; [i] PhpHR (2018). 'Serbian Police Arrest Suspected Hacker Connected to "The Dark Overlord"', linksoftvn.com, 17 May: *http://linksoftvn.com/serbian-police-arrest-suspected-hacker-connected-to-the-dark-overlord/*; [j] Exit Brief (2017). 'Anonymous Albania Threatens Government and Media with Further Attacks,' exit: Explaining Albania, 11 July: *https://exit.al/en/2017/07/11/anonymous-ALBANIA-threatens-government-and-media-with-further-attacks/*; [k] Organized Crime and Corruption Reporting Project (OCCRP) (2016). 'Bosnia and Herzegovina: Crackdown on "Cyber Blackmail" Group', 13 Jan.: https://www.occrp.org/en/component/content/article?id=4793:bosnia-and-herzegovina-crackdown-on-cyber-blackmail-group; [l] Amir, W. (2012). 'US Weather.Gov Hacked, Data Leaked by Kosova Hacker's Security', HackRead, 20 Oct.: *https://www.hackread.com/us-weather-gov-hacked-data-leaked-by-kosova-hackers-security/*.

34 This is not an exhaustive list. It represents a range of attacks that received media coverage between 2013 and 2018. A formal list of incidents is not available.

35 "Eco Tirana sh.a was born from the need to give local public administration a company organised in accordance with high standards of quality and efficiency, through the use of advanced management techniques as well as use of latest technology vehicles and equipment; makes possible the good management of the Albanian capital for the urban hygiene service and the differentiated collection of waste, according to the best international standards". See *http://www.ecotirana.com*.

2. EUROPEAN ENVIRONMENT

This report supplies an overview of the situation in the WB6 with respect to cyber security. During the research phase, it was immediately clear that much of what is driving WB6 government activity in this area, especially with regard to legislation, strategies, and policies, is EU activity. In fact, the EU legal framework is probably the most influential on the WB6. For economies looking to join the EU, harmonisation in this area is viewed as important. This is not the sole reason for the WB6's concern with cyber security issues, of course; there is also recognition that there are considerable risks associated with failing to adequately address issues arising in this area, evident in the RCC MAP and the Western Balkans Digital Agenda. This section highlights a number of the key elements of the EU's cyber security framework, along with other influential actors and policies. These include, the Cyber Security Strategy of the European Union, the Network and Information Security (NIS) directive, Budapest Convention on Cybercrime, Digital Agenda for Europe (DAE), ENISA, NATO, Council of Europe, OSCE, and International Telecommunication Union (ITU). The purpose of the section is to supply context for and highlight some of the influences on the WB6's cyber security posture, which will be detailed in section 4.

2.1 Cyber Security Strategy of the European Union

The EU published its Cyber Security Strategy in 2013 in the context of a growing recognition that an open and free cyberspace "promoted political and social inclusion worldwide".[34] The strategy notes that "the borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation".[35] The EU also highlights in the strategy the role ICT plays in relation to economic growth, stating that "by completing the Digital Single Market, Europe could boost its GDP by almost €500 billion a year".[36] Nonetheless, they recognised the need for citizens to have trust and confidence in digital infrastructure for this to be achieved. Such trust and confidence is not where it should be. According to the special 2015 Eurobarometer survey (No. 423) on cyber security, the two most common concerns for those using the internet were in relation to someone misusing their personal data (mentioned by 43%) and security of online payments (42%). Only 18% of respondents said they had no concerns about using the internet for things like online banking or buying things online. These percentages were all increased since a similar survey in 2013.[37]

The strategy also clarifies the principles that should guide cyber security policy, both in the EU and internationally. It notes that the EU's core values, such as its laws and norms, apply both to the physical world and the digital world. It identifies the need for cyber security to protect fundamental rights, freedom of expression, personal data, and privacy, whilst being accessible to all. The strategy recognises that the digital world is not controlled by a single entity, and as a result, reaffirms and supports a multi-stakeholder governance approach, to include the public sector, private sector, and individual users, who all share responsibility to strengthen cyber security.[38] The strategy includes five strategic objectives, namely (i) achieving cyber resilience; (ii) drastically reducing cybercrime; (iii) developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP); (iv) developing the industrial and technological resources for cyber security; and (v) establishing a coherent international cyberspaces policy for the EU, including promoting core EU values and setting out how they will be achieved.

One key aim of the strategy is to establish common minimum standards across Member States. This is deemed important as systems are only as strong as the weakest link. The strategy also identifies key partners both at the national and EU level. They do this under three pillars, the Network and Information Security Directive (NIS), law enforcement, and defence, whilst also identifying the role of industry and academia at each level. Setting out the roles and responsibilities of such parties is important, given the acknowledgment that the strategy's "vision can only be realised through partnership, between actors, to take responsibility and meet the challenges ahead".[39]

It is not possible to discuss the strategy in detail, as the document references a large number of key activities and agencies envisaged to be involved in the implementation of the strategy. That said, some aspects mentioned in the strategy will be discussed further such as NIS, the Council of Europe Convention on Cybercrime, commonly known as the Budapest Convention, and the European Network and Information Security Agency (ENISA). Before doing that a number of other relevant EU Strategy Documents will be highlighted.

2.1.1 Other EU Strategy Documents

Three other strategic documents important in the cyber security realm are the European Agenda on Security (2015), the Digital Single Market Strategy (2015), and the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cyber Security Industry (2016). The European Agenda on Security 2015 – 2020 sets out the following actions in relation to cybercrime:

[G]iving renewed emphasis to implementation of existing policies on cybersecurity, attacks against information systems, and combating child sexual exploitation; reviewing and possibly extending legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016; reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information; enhancing cyber capacity building action under external assistance instruments.[40]

The Digital Single Market Strategy (2015) recognises the need for trust and security in order to reap the benefits of the digital economy. As a result, it includes reference to a:

Public-private partnership (PPP) on cybersecurity. The goal of this partnership is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions. [41]

The Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cyber Security Industry (2016) sets out measures aiming to:

34 European Commission (2013). *Cyber Security Strategy of the European Union*, p.2.

35 European Commission (2013). *Cyber Security Strategy of the European Union*, p.3.

36 European Commission (2013). *Cyber Security Strategy of the European Union*, p.3.

37 European Commission (2015). *Special Eurobarometer 423: Cyber Security*, Brussels: Directorate-General for Home Affairs and Directorate-General for Communication, Feb., p. 2: *http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf*.

38 European Commission (2013). *Cyber Security Strategy of the European Union*, p.4.

39 European Commission (2013). *Cyber Security Strategy of the European Union*, p.19.

40 European Commission (2017). 'Fact Sheet: EU Cybersecurity Initiatives – Working Towards a More Secure Online Environment', p.2: *http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf*.

41 European Commission (2017). 'Fact Sheet: EU Cybersecurity Initiatives', p.3.

Step up cooperation across Europe: the Commission encourages Member States to make the most of the cooperation mechanisms under the NIS Directive and to improve the way in which they work together to prepare for a large-scale cyber incident. This includes more work on education, training and cybersecurity exercises; support the emerging single market for cybersecurity products and services in the EU: for example, the Commission will explore the possibility of creating a framework for certification of relevant ICT products and services, complemented by a voluntary and light weight labelling scheme for the security of ICT products; the Commission suggests also possible measures to scale up cybersecurity investment in Europe and to support SMEs active in the market; establish a contractual public-private partnership (PPP) with industry, to nurture cybersecurity industrial capabilities and innovation in the EU.[42]

Together, these documents illustrate the breath of policy areas influencing the cyber security agenda in the EU, while also illustrating that the EU has a largely narrow and traditional view of what constitutes cyber security, emphasising attacks and cybercrime.

2.2 EU Legislation

2.2.1 Network and Information Security Directive (NIS)

The Network and Information Security Directive[43] (NIS) was the first piece of EU-wide cyber security legislation and was strongly referenced throughout our field research. The aim of the directive is to enhance cyber security across the EU by laying down "measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market".[44] Since its adoption in 2016, EU Member States were required to transpose the NIS into their national legislation.[45] The deadline for this was 9 May 2018, but not all Member States met this deadline.[46] The NIS has three key components, which relate to national cyber security capabilities, cross-border collaboration, and national supervision of critical sectors. According to the NIS, Member States should equip themselves with cyber capabilities such as a national strategy on the security of network and information systems, a national competent authority and single point of contact, a national CSIRT, support national cooperation, and should perform cyber exercises. Secondly, the NIS highlights the need for international cooperation. The NIS Cooperation Group,[47] which is described in Article 11 of the directive, is mentioned in this context. The Group is composed of representatives of relevant national ministries and national cyber security agencies, the European Commission, and ENISA. EU Member States cooperate, exchange information and agree on continuity and consistency of implementation of the directive within the Group. It also provides strategic direction to the EU CSIRT network, which is also a cross-border collaboration.

Thirdly, the NIS also asserts that EU member states should supervise operators of essential services. The criteria for identification of such operators are set out in Article 5 of the directive as follows:

(a) An entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.[48]

Member states must provide *ex-ante* supervision of critical market operators, such as the energy, transport, drinking water supply and distribution, health, and finance sector, and *ex-post* supervision for critical digital service providers (e.g. internet exchange points, domain name systems, etc.).[49] The NIS also details obligations regarding security requirements, incident notification, and implementation and enforcement for both groups.

The NIS encourages the use of standardisation and voluntary notification. ENISA assists in this task by (i) identifying good practices in the Member States regarding the implementation of the NIS directive, (ii) supporting the EU-wide cyber security incident reporting process, by developing thresholds, templates and tools, (iii) agreeing on common approaches and procedures and (iv) helping Member States to address common cyber security issues. The NIS also states that Member States "shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented".[50]

While the NIS remains one of the main legal instruments underpinning EU cyber security, in September 2017 the Commission proposed a new cyber security policy initiative to enhance its cyber resilience. This has become known as the Cyber Security Act. It includes a recommendation for EU Member States to develop a framework for the exchange of cyber security information, a proposal for an EU-wide cyber security certification framework, and a proposal for a stronger mandate for ENISA, so that it can become "a true EU Cybersecurity agency".[51] This legislation also envisages establishment of a permanent EU agency for cyber security, which would be given new tasks in supporting Member States, EU institutions, and other key stakeholders in this area. Other obligations will include organising regular EU-level cyber security exercises, and supporting and promoting EU policy on cyber security certification.

The importance of the NIS, in particular, was recognised in the interviews we conducted. It appeared to be the driving influence on the WB6's approach to cyber security and a fundamental underpinning of their legislative frameworks.

2.2.2 Other EU legislation

- A variety of other EU legislation relevant in the cyber security is worth briefly mentioning here too, including:
- The EU General Data Protection Regulation (GDPR) which came into effect on 25 May 2018. It replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy;[52]
- Directive 2013/40/EU on Attacks Against Information Systems aims to tackle large-scale cyber attacks by requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions;[53]
- Directive 2011/92/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography addresses online child sexual exploitation, including online grooming;[54]

The Framework Decision on Combating Fraud and Counterfeiting of Non-cash Means of Payment (2001) defines the fraudulent behaviours, including online activities that EU States need to consider as punishable criminal offences.[55]

2.3 The Budapest Convention on Cybercrime

Another important document is the Budapest Convention on Cybercrime (2001), which was the first international treaty to focus specifically on crimes committed via the internet and other computer networks. It provides a legal framework for combating cybercrime, including attacks against information systems.[56] It also addresses issues such as infringements of copyright, computer-related fraud, child sexual exploitation material, hate crimes, and violations of network security. The convention

42 *Ibid.*

43 Council Directive 2016/1148/EU Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 6 July: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN*.

44 Council Directive 2016/1148/EU Concerning Measures for a High Common Level of Security of Network and Information Systems, p.3.

45 EU directives do not have to be uniformly transposed into national legislation. There is some level of flexibility given that national circumstances can differ.

46 On 19 July 2018, the EC notified 17 Member States of their failure to implement the EU cyber security legislation within the timeframe. These were Austria, Bulgaria, Belgium, Croatia, Denmark, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, and Spain.

47 Since its establishment the NIS Cooperation Group has published seven working documents. These are CG Publication 01/2018, 'Reference Document on Security Measures for Operators of Essential Services'; CG Publication 02/2018, 'Reference Document on Incident Notification for Operators of Essential Services (Circumstances of Notification)'; CG Publication 03/2018, 'Compendium on Cyber Security of Election Technology'; CG Publication 04/2018, 'Cyber Security Incident Taxonomy'; CG Publication 05/2018, 'Guidelines on Notification of Operators of Essential Services incidents (Formats and Procedures)'; CG Publication 06/2018, 'Guidelines on Notification of Digital Service Providers incidents (Formats and Procedures)'; CG Publication 07/2018, 'Reference Document on the Identification of Operators of Essential Services (Modalities of the Consultation Process in Cases with Cross-border Impact)'. All of these are available at the following URL: *https://ec.europa.eu/digital-single-market/en/nis-cooperation-group*.

48 Council Directive 2016/1148/EU (2016) Concerning Measures for a High Common Level of Security of Network and Information Systems, p.14.

49 See *https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive*

50 Council Directive 2016/1148/EU (2016) Concerning Measures for a High Common Level of Security of Network and Information Systems, p.24.

51 See the dedicated ENISA Webpage on the 'NIS Directive': *https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive*.

52 Available online at *https://eur-lex.europa.eu/eli/reg/2016/679/oj*.

53 Available online at *https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32013L0040*.

54 Available online at *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093*.

55 Available online at *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001F0413*.

56 Minovic, A., Abusara, A., Begaj, E., Erceg, V., Tasevski, P., Radunović, V., and Klopfer, F. (2016). *Cyber Security in the Western Balkans: Policy Gaps and Cooperation Opportunities*, Geneva: Diplo Foundation: *https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf*.

resulted from recognition by signatories that it was necessary "to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation".[57] It requires parties "to adopt appropriate legislation against cybercrime; ensure adequate procedural tools to effectively investigate and prosecute cybercrime offences; and to provide international co-operation to other parties engaged in such efforts".[58] The Convention also recognises the need for cooperation between states and private industry in combating cybercrime. It promotes the need for better international police and judicial cooperation in the area of cybercrime, reinforced through the creation of a 24/7 network. This required every party to:

[D]esignate a point of contact available on a twenty-four hour, seven-days-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[59]

According to Article 38 of the Convention:

(i) Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply. (ii) Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General; (iii) Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe.[60]

Five of the WB6 are part of the convention, with the exception of Kosovo*. However, all six have appointed a 24/7 point of contact. While the benefits (e.g. 'real time' interaction in cybercrime cases) of the 24/7 contact were acknowledged in interviews we undertook, it was highlighted that where evidence needs to be accessed and exchanged, mutual legal assistance protocols take precedence, which can be time consuming and often negatively impact progress. Unsurprisingly, it was noted too that some national points of contact were more willing to cooperate than others. Nonetheless, the Budapest Convention has clearly impacted the WB6's approach to securing cyberspace.

2.4 The Digital Agenda for Europe (DAE)

A key document that views cyberspace from a perspective of opportunity rather than risk is the Digital Agenda for Europe (DAE). The DAE was adopted in 2010 and is one of seven flagship initiatives under the Europe 2020 strategy. The key aim of the DAE is "to deliver sustainable economic and social benefits from a digital single market based on fast and ultrafast internet and interoperable applications".[61] Its main objective is "to chart a course to maximise the social and economic potential of ICT, most notably the internet, a vital medium of economic and societal activity: for doing business, working, playing, communicating and expressing ourselves freely".[62] The DAE has seven priority areas for action, namely (i) creating a digital Single Market; (ii) greater interoperability; (iii) boosting internet trust and security, (iv) much faster internet access; (v) more investment in research and development; (vi) enhancing digital literacy skills and inclusion; and (vii) applying information and communications technologies to address challenges facing society, like climate change and the ageing population. When published, the DAE outlined 100 specific follow-up actions to achieve its goals, which included 31 legislative proposals.[63]

In June 2013, the EU underlined the role of the DAE by:

"(i) Reiterating its call to complete the digital single market by 2015; (ii) pointing to the need to address overdue investment needs in telecoms infrastructure; (iii) calling for the promotion of the right skills for the modern economy; (iv) stressing the importance of working with our partners to fight cybercrime".[64]

The DAE has achieved successes. For example, the Digital Single Market Strategy for Europe was adopted in May 2015, around three pillars. These include better access for consumers and businesses to online goods and services across Europe, creating the right conditions for digital networks and services to flourish, and maximising the growth potential of the European Digital Economy. Two important elements for achieving this, as mentioned above, are trust and security, without which the DAE or the Digital Single Market will not be effective. The majority of our interviewees noted that the commitments made in these strategies, including trust and security as key components, are of growing importance in the WB6 given the number of citizens conducting business and commercial transactions online is continually increasing, coupled with the increased prioritisation of e-government services. This was illustrated in the work of the CSIRTs. For example, the national CSIRT of Albania was described as very proactive in the area of cyber security awareness raising.

2.5 The European Union Agency for Network and Information Security

The EU acknowledges that legislation, strategies, and aspirations cannot be effective without proper resourcing. As a result, ENISA was established in 2004 to contribute to achieving the EU's goals relating to network and information security. ENISA is the centre of expertise for cyber security in Europe and has, since its establishment, been developing a culture of network and information security across the EU. ENISA supports the Commission, Member States, and the private sector to address, respond, and prevent information security related incidents. ENISA's key activities include (i) collecting and analysing data on security incidents in Europe and emerging risks, (ii) promoting risk assessment and risk management methods to enhance capability to deal with information security threats, (iii) running of pan-European cyber exercises, (iv) supporting Computer Emergency Response Teams (CSIRTs) cooperation in the Member States, (v) awareness-raising and cooperation between different actors in the information security field.

ENISA mainly delivers advice and solutions. Examples of this include organising, in conjunction with the single points of contact in Member States, a cyber security awareness campaign every October to draw attention to cyber security issues in the EU. ENISA also conducts:

Pan-European Cyber Security Exercises, provides support in the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, e-IDs and trust services, and identifying the cyber threat landscape, and others.[65]

Our interviewees mentioned ENISA largely in reference to training and support offerings. One highly commended aspect of ENISA training related to the crisis exercises they run. However, some national CSIRTs highlighted that they cannot access some of these exercises as they are not yet EU members, saying they would benefit even if allowed to observe, given the exercises quality and relevance.[66]

2.5.1 EU Computer Emergency Response Team (CSIRT-EU)

Despite Member States having national CSIRTs, the EU Computer Emergency Response Team (CSIRT-EU) was established in 2012. The aim of CSIRT-EU is "to provide effective and efficient response to information security incidents and cyber threats for the EU institutions, agencies and bodies".[67] Experts in the unit are drawn from the European Commission, the General Secretariat of the Council, the European Parliament, the Committee of the Regions, and the Economic and Social Committee. CSIRT-EU cooperates with CSIRTs in the Member States and further afield. It also cooperates with the private sector, through connections with specialised IT security companies.

2.5.2 Europol's Cybercrime Centre

Europol's Cybercrime Centre (EC3) was established in 2013. The centre acts as:

"A focal point in combatting and preventing cross-border cybercrime by: serving as the central hub for criminal information and intelligence; supporting Member States' operations and investi-

57 Council of Europe (2001). *Convention on Cybercrime*, Budapest: Council of Europe, p.2: *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf*.

58 Council of Europe (2001). *Convention on Cybercrime*, p.8.

59 Council of Europe (2001). *Convention on Cybercrime*, p.20.

60 Council of Europe (2001). *Convention on Cybercrime*, p.22.

61 European Commission (2010). *A Digital Agenda for Europe*, Brussels: European Commission, p.3: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN*.

62 *Ibid*.

63 More details on these activities is available in European Commission (2010). 'Digital Agenda for Europe: Key Initiatives', *Press Release*, 19 May: *http://europa.eu/rapid/press-release_MEMO-10-200_en.htm?locale=en*.

64 European Commission (2014). *The European Union Explained: Digital Agenda for Europe*, Luxembourg: Publications Office of the EU, p.7: *http://eige.europa.eu/resources/digital_agenda_en.pdf*.

65 From the 'About' section of ENISA's official website at *https://www.enisa.europa.eu/about-enisa*.

66 RB17 interviewed between 11 June and 21 June 2018 in Sarajevo, BiH.

67 European Commission (2017). 'Fact Sheet: EU Cybersecurity Initiatives', p.5.

gations by means of operational analysis, coordination and expertise; providing strategic analysis products; reaching out to cybercrime related law enforcement services, private sector, academia and other non-law enforcement partners (such as internet security companies, the financial sector, computer emergency response teams) to enhance cooperation amongst them; supporting training and capacity building in the Member States; providing highly specialised technical and digital forensic support capabilities to investigations and operations; representing the EU law enforcement community in areas of common interest (R&D requirements, internet governance, policy development).[68]

Europol's Internet Referral Unit (EUIRU), which detects and investigates malicious content on the internet and in social media, particularly jihadi online content,[69] is a component of Europol's European Counter Terrorism Centre (ECTC) and not EC3.

2.6 Additional Programmes and Activities

The EU has proactively sought to coordinate its activities with international activities in the area of cyber security. For example, the EU and Member States engage in policy dialogue with international partners and with international organisations such as the Council of Europe, the Organization for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), and the United Nations (UN). A number of these programmes and activities were mentioned by respondents as impactful. These included the United Nations (IPA), the CoE's iProceeds programme, the work of the OSCE, and the work of the International Telecommunication Union (ITU). Each of these is discussed in brief below.

2.6.1 NATO

NATO adopted a policy and action plan on cyber defence in September 2014. This established cyber defence as part of the alliance's core tasks. It also confirmed that international law applies to cyberspace, which enables NATO to work more closely with industry, especially in the area of information sharing, the exchange of best practices, and exploration of new and emerging technologies. A top priority for NATO in this area is the "protection of the communications and information systems owned and operated by the Alliance".[70] The policy provides for "streamlined cyber defence governance procedures for assistance to Allied countries in response to cyber attacks, and the integration of cyber defence into operational planning, including civil emergency planning". It does this through awareness raising, education, and cyber exercises. It also encourages cooperation initiatives with partner countries and international organisations. In 2014, NATO established a Computer Incident Response Capability (NCIRC), which protects NATO's own networks by providing centralised and round-the-clock cyber defence support to various NATO sites. It is supported by a number of rapid reaction teams. Similar to other CIRTS, NCIRC analyses and reports incidents, and disseminates important incident-related information to system/security management and users. NATO's cyber security work was identified by interviewees as critical, with many commending training they had received. Similar to ENISA, NATO's cyber coalition exercises were highly valued by those who attended. However, similarly to ENISA, the non-NATO economies (i.e. Bosnia and Herzegovina, Kosovo,* The Former Yugoslav Republic of Macedonia, Serbia) highlighted that they cannot access some exercises.

2.6.2 CyberCrime@IPA and iProceeds

CyberCrime@IPA is the short title for the project 'Regional Co-operation in Criminal Justice: Strengthening Capacities in the Fight against Cybercrime', which was a joint regional project of the European Union and the Council of Europe under the IPA that ran from 2010 to 2013. All WB6 economies were beneficiaries, along with Croatia and Turkey. 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".[71] This project has been over for five years, but it is recognised for having had a positive impact in the WB6. iProceeds is also a joint project between the EU and the CoE, which commenced in 2016 and will run until June 2019, and of which again all WB6 economies are beneficiaries, along with Turkey. The objective of this programme is to "strengthen the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet".[72]

Both programmes were commended and valued by our interviewees for the support provided. Some criticisms were levelled against them however, including that while twinning projects were useful with regard to mentoring and expert support, the WB6 often lacked support for the logistical component necessary to get the best out of the opportunity. In respect to iProceeds, the training was deemed very good, but as expertise and knowledge improve, training needs also to increase especially in regard to more contextual issues; this additional training was felt to be deficient.

2.6.3 OSCE

The role of the OSCE in the area of cyber security within the region was recognised by respondents. Two aspects of their role were deemed particularly relevant to the WB6; these are the OSCE's emphasis on regional cooperation and the promotion of public-private partnerships, including at the national level. Particular praise was attached to the OSCE's ability to bring a wide range of stakeholders together, something described as often absent from other programmes. Their work in Serbia was utilised as a case in point, which may be a model for the region. The establishment of an informal network of IT professionals and related stakeholders was initiated by OSCE around three years ago, and implemented by the Diplo Foundation and the Geneva Centre for the Democratic Control of Armed Forces (DCAF). This network has grown since then and is now an excellent example of how such networks can help to enhance the field in a sustainable manner, even where there is a lack of resources and the necessary strategic thinking. The group has been influential in shaping and steering law and strategy development at the national level, as well as bringing together stakeholders from the public and private sectors to support each other's work. This has been achieved, in part, by creating an environment of trust and cooperation between all parties with a shared commitment to, enthusiasm for, and vision of where things need to be.

2.6.4 International Telecommunication Union (ITU)

Lastly, the work of the ITU was also highlighted. The ITU is the United Nations' (UN) specialised agency responsible for issues that concern information and communication technologies (ICTs). Since its establishment in 1865 it has produced a wide array of security frameworks, architectures, and standards. With a membership of 193 countries and almost 800 private-sector entities and academic institutions, the ITU's structuring is a prime example of a successful public-private partnership approach. In 2008, the ITU partnered with a consortium of institutions and organisations called the International Multilateral Partnership against Cyber Threats (IMPACT). This alliance seeks 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 cyber security strategies and critical infrastructure protection, to enhance coordination and cooperation in securing cyberspace".[73] Four of the WB6, namely Albania, Bosnia and Herzegovina, Montenegro, and Serbia are partner economies of the alliance. ITU-IMPACT provides technical, non-technical, and capacity building related services, which was considered by those we interviewed who were involved with it to have real value.

2.7 Funding

The EU's progress in cyber security could not be achieved without considerable funding. Between 2007 and 2013, the EU invested €334 million in cyber security and online privacy projects in the form of research and innovation under programmes such as the 7th Framework Programme (FP7) and the Competitiveness and Innovation Programme (CIP).[74] This has continued, since 2014, under the Horizon 2020 Research and Innovation Framework Programme (H2020). Between 2014 and 2020 the EU is expected to invest a further €450 million in the area under two streams, digital security and the fight against crime and terrorism. During the same period, it is envisaged that the European Structural and Investment (ESI) Funds will also contribute up to €400 million for investments in trust and cyber security.

The EU has also invested in Digital Service Infrastructures (DSIs). This has occurred under the ambit of the Connecting Europe Facility (CEF), the aims of which are achieving "cross-border cooperation in cyber security, enhancing the security and thus

68 *Ibid.*

69 From the 'About' section of Europol's official website at *https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru*.

70 NATO (2016). 'Fact Sheet: NATO Cyber Defence', p. 1: *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf*.

71 From the project's dedicated webpage on the CoE's official website: *https://www.coe.int/en/web/cybercrime/cybercrime-ipa*.

72 From the project's dedicated webpage on the CoE's official website: *https://www.coe.int/en/web/cybercrime/iproceeds*.

73 Ntoko, A. (2011). 'Global Cybersecurity Agenda (GCA): A Framework for International Cooperation', presentation at the Open-ended Intergovernmental Expert Group on Cybercrime, Vienna, 17-21 Jan., p.18: *https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf*.

74 European Commission (2017). 'Fact Sheet: EU Cybersecurity Initiatives'.

the trust in cross-border electronic communication, contributing to the creation of the Digital Single Market".[75] CEF also undertakes dedicated projects against cybercrime, while the Commission covers Europol EC3's staff and operational costs and the financing for the Internal Security Fund (ISF). ISF funding is available for setting up and running IT systems, acquisition of operational equipment, promoting and developing training schemes, and ensuring administrative and operational coordination and cooperation. This section on funding is not exhaustive, but it provides insight into the amount and nature of support given by the EU to ensure implementation of its cyber security priorities.

Overall, this section serves to illustrate the wide array of actions and activities conducted by the EU in the area of cyber both from the perspective of risk and opportunity. While the section cannot include all the activities due to its scale and scope, the examples discussed show the multi-layered approach the EU has taken to maximise opportunities while minimising risks. The next section will examine how such activities and actions have influenced developments within the WB6.

75 European Commission (2017). 'Fact Sheet: EU Cybersecurity Initiatives', p. 6.

3. CYBER SECURITY IN THE WESTERN BALKANS

This section details progress made and continuing challenges within the WB6 in respect to cyber security. The influence of the EU is further discussed in the first half of this section in the context of the influence of its legislation policies, strategies, and activities on the WB6's economies cyber security postures. Operational level progress has been less pronounced however. The issues that hinder this area of progress are discussed in the second half of this section.

3.1 Legislation, strategies, and policies

The WB6 are actively formalising their cyber security legislation and harmonising it with the EU's framework. Legislation pertaining to cyber security is present in all the WB6, with the exception of Bosnia and Herzegovina at the state level where legislation is present at the entity level. In addition to legislation, three of the WB6, Serbia, Kosovo,* and Montenegro, have cyber security strategies in place at central government level. Bosnia and Herzegovina does not have a strategy at the state level, whilst The Former Yugoslav Republic of Macedonia has adopted a new strategy for the period 2018-2022 with action plan under preparation. Albania does not have a strategy *per se*, the 'Paper on Cyber Security 2015 – 2017' acts in lieu. Additionally, whilst Serbia has a strategy it does not have a corresponding action plan as of yet. The remaining economies, Kosovo,* and Montenegro have both cyber security strategies and accompanying action plans, with Montenegro in its second iteration. Further to this, the WB6 have a range of other legislation applicable to the field of cyber security. Table 5 identifies a selection of this legislation, which is being developed and adopted in light not just of a desire for harmonisation with the EU cyber security framework, but also in order to make WB6 markets more attractive for investment.

Table 5. Additional cyber security legislation within WB6 economies[78]	
ALBANIA	Cross-cutting Strategy on Information Society (CSIS) 2008-2013
	Law on Protection of Children's Rights and the Action Plan on Children 2012-2015
	Code of Conduct for the Safer and Responsible Use of Electronic Communications Networks and Services
	Decision of the Council of Ministers No. 973 "On approval of Cyber Security Document 2015 – 2017"
	Law No. 2/2017 on Cyber Security
	Decision of the Council of Ministers No. 141 2017, "On organising and functioning of national authority for electronic certification and cybersecurity"
BOSNIA AND HERZEGOVINA	Law on Communications
	Law on Electronic Signature
	Law on Electronic Legal and Business Transactions
	Law on Prevention of Money Laundering and Financing of Terrorism
KOSOVO*	Law on Prevention and Fight against Cybercrime
	Law on Electronic Communication
	Police Law - Standard Operating Procedures
	National Cyber Security Strategy
MONTENEGRO	Law on Information Security
	Regulation on Information Security Measures
	Law on Ratification of the Convention on Cybercrime
	Law on Ratification of Protocol to the Convention on Cybercrime
	Law on Electronic Communications
	Law on Liability of Legal Persons for Criminal Acts
	Law on the Implementation of Regulations Governing the Protection of Intellectual Property Rights
	Law on Personal Data Protection
SERBIA	Law on Ratification of the Convention on Cybercrime
	Law on Ratification of Protocol to the Convention on Cybercrime
	Law on Electronic Media
THE FORMER YOGOSLAV REPUBLIC OF MACEDONIA	Law on Interception of Communication
	Law on Electronic Communications
	Law on e-Commerce
	Law on Electronic Management
	Law on Data in Electronic Form and Electronic Signature
	Law on Personal Data Protection
	Law on Free Access to Public Information

76 The following web link provides a list of Council of Europe's conventions where one can see those ratified per economy. *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=QdQ70zbA*

3.2 Regional Development Agenda

Commitment in the area of cyber in the WB6 stretches beyond security and mitigating associated risks to support economic growth and regional development. This is illustrated by the Multi-annual Action Plan for a Regional Economic Area in the Western Balkans (MAP), which was developed in 2017[77], upon the request of the WB6's Prime Ministers to further economic cooperation and growth in the region. The MAP sets out a structured agenda for regional economic integration, by "promoting further trade integration, introducing a dynamic regional investment space, facilitating regional mobility, and creating a digital integration agenda".[78] Progress has been achieved in respect to the digital agenda:

[The] region has initiated structured high-level regional political dialogue on WB6 digitisation through Annual WB Digital Summits, with the 1st WB Digital Summit held in Skopje on 18 – 19 April 2018; RCC networked the Computer Security Incident Response Team (CSIRTs) from WB6 and extended capacity building to their representatives thus strengthening cyber security capacities and enhancing regional cooperation among WB6 CSIRTs.[79]

This illustrates that a similar perspective to that in the EU is also opened within the WB6, particularly a growing recognition for the need to strike a balance between the opportunities offered by ICT and the risks this brings.

The EU is also providing tangible support to this transformation within the region, in recognition of its importance in the EU accession process. An example of this support relating to cyber security is the EC's launch of the Digital Agenda for the Western Balkans, which took place in June 2018. The launch of the Digital Agenda is one of six[80] initiatives designed to support the transformation of the Western Balkans. A second initiative designed to increase connectivity also focuses, in part, on cyber security, given the recognition that better physical and cyber connectivity will increase competitiveness, economic growth and security of supply. The digital agenda involves five areas of action:

[A] roadmap to facilitate lowering roaming costs; support to the deployment of broadband; the development of eGovernment, eProcurement, eHealth and digital skills; capacity building in digital trust and security in parallel to efforts enhancing the digitalisation of industries; and enhanced support for the adoption and implementation of the acquis.[81]

This summit was a precursor to the May 2018 'Sofia Declaration', which was agreed by the leaders of the EU and Member States, in consultation with Western Balkans partners. In this they concluded that "disinformation and other hybrid activities will be fought together through greater collaboration in resilience, cyber security and strategic communication".[82] This is indicative that both the EU and WB6 partners want to be forward thinking in their understanding of cyber security, looking beyond the traditional narrow understanding to include elements like disinformation and other hybrid activities. This is further recognition of the need for policy makers, programme developers, and other stakeholder in this field to consider a broader conception of cyber security going forward.

The presence of these documents, declarations, and action plans alone should not, of course, be viewed as indicative of significant progress in cyber security. While their development and adoption is positive, it seems that implementation of the strategies has not kept pace with legislative developments. This is evident from the 2018 EU assessments of the WB6 carried out by the European Commission (see Table 6). Despite recognition of the importance of having appropriate legislation in place, the importance of the allied operational capacities in the cyber security domain is not yet seen as a priority in the WB6. There is an observable mismatch between words and deeds in respect to cyber security in the region, in other words. The next sub-section will examine this further.

77 The time frame is 2017 to 2020, with some actions extending until 2023.

78 RCC (2018). 'Multi-Annual Action Plan for a Regional Economic Area in the Western Balkans'.

79 European Commission (2018). 'European Commission Launches Digital Agenda for the Western Balkans'.

80 Other initiatives include those on strengthening the rule of law, reinforcing engagement on security and migration, enhancing support for socio-economic development, increasing connectivity, and supporting reconciliation and good neighbourly relations.

81 European Commission (2018). 'EU-Western Balkans: Six Flagship Initiatives': https://ec.europa.eu/commission/sites/beta-political/files/six-flagship-initiatives-support-transformation-western-balkans_en.pdf.

82 EU-Western Balkans Summit (2018). 'Sofia Declaration', 17 May, p.3: http://www.consilium.europa.eu/media/34776/sofia-declaration_en.pdf.

Table 6. EU Assessments 2018 under Chapter 10 and 24 of the Acquis	
ALBANIA	In regard to Chapter 24 and obligations in respect to information security, Albania is moderately prepared. Some progress had been made in relation to the digital agenda action plan and e-government services. The cross-sectoral strategy on Albania's digital agenda for 2015-2020 and the plan for broadband development are being implemented, whilst the Law on Cyber Security is partly aligned with the NIS. The assessment notes that there has been good progress in the area of electronic communications with approval of the law on development of high-speed electronic communication networks and the provision of the right of way, stating that this law fully complies with the acquis. However, the assessors state that Albania needs to develop a national cyber security strategy.[a]
BOSNIA AND HERZEGOVINA	Bosnia and Herzegovina lacks a strategic framework to address the issue of cybercrime and cyber security threats. Investigations in cybercrime reportedly remain very rare. The assessment notes that "the existing capacity to combat cybercrime (including addressing on-line child sexual abuse material) and to effectively respond to cyber security threats need to be strengthened".[b] It assessed that a number of specialised investigation units, including those relating to cyber security, have insufficient capacity. While not specifically referring to cyber security, the report noted that the legal framework to fight organised crime is only partially aligned with the EU acquis and that BiH's digitalisation was reported to be still at a very low level.
KOSOVO*	Kosovo* has made some very positive progress in regard to cyber security. The report noted that, in general, the Kosovo's* cybercrime legislation is in line with the EU acquis. However, it did note that "alongside planned changes to the Criminal Code, the authorities should ensure a proper conclusion to the ongoing revision of the Law on Prevention and Fight of Cybercrime, taking into account the available expertise of the international community".[c]
MONTENEGRO	The EU assessment report of Montenegro did not include a substantive evaluation in relation to cyber and cyber security. In relation to chapter 10, the EU assessed that there is good functioning of the internal market for electronic communications and electronic commerce and audio-visual services. However, overall it assesses that Montenegro continues to be moderately prepared in the area of information society. In relation to chapter 24, the EU assessed that Montenegro is moderately prepared to implement the acquis in this area. They noted that the legal and strategic frameworks are now largely in place. They further note that investigations into cybercrime, including online child sexual abuse, remain very rare. This was reiterated in interviews in Podgorica. [d]
SERBIA	At the time of the assessment, Serbia had yet to adopt a strategy on cybercrime, a recommendation of the assessment. Furthermore, full harmonisation of the law on information security with the NIS is still pending. Under Chapter 24, the operational capacity in the Prosecutor's Office for Cybercrime was reported as improved. Under Chapter 10, Serbia is described as moderately prepared in the field of information society. Progress was reported "in the field of electronic communications and information and communication technologies, with the adoption of a law on e-document, e-identification and trust services in e-business, in line with the acquis".[e] However, a law on electronic communications aimed at alignment with the 2009 EU regulatory framework, as well as a law on broadband and the Next Generation Networks Strategy, to be based on the EU's Digital Agenda, have yet to be adopted.
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA	The Criminal Code of The Former Yugoslav Republic of Macedonia is broadly in line with European standards, criminalising online child sex abuse and computer crime, amongst other crimes. In relation to Chapter 10, the assessors note that The Former Yugoslav Republic of Macedonia still does not have a dedicated National Cyber Security Strategy and includes that in their recommendations. Preparation of a long-term Information Communication Technology (ICT) Strategy is also recommended. The assessment notes that The Former Yugoslav Republic of Macedonia is moderately prepared to implement the acquis under Chapter 24, but does not specifically mention cybercrime.[f]

Sources [a] European Commission Staff (2018). *Albania 2018 Report*, Strasbourg, 17 April, p. 24: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-albania-report.pdf*.; [b] European Commission Staff (2018). *Bosnia and Herzegovina 2018 Report*, Strasbourg, 17 April, p. 23: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-bosnia-and-herzegovina-report.pdf*; [c] European Commission Staff (2018). *Kosovo* 2018 Report*, Strasbourg, 17 April, p.29: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-kosovo-report.pdf*; [d] European Commission Staff (2018). *Montenegro 2018 Report*, Strasbourg, 17 April, p. 29-31: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-montenegro-report.pdf*; [e] European Commission Staff (2018). *Serbia 2018 Report*, Strasbourg, 17 April, p.63: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-serbia-report.pdf*; [f] European Commission Staff (2018). *The Former Yugoslav Republic of Macedonia 2018 Report*, Strasbourg, 17 April, p. 33: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-the-former-yugoslav-republic-of-macedonia-report.pdf*.

3.3 Challenges to operational implementation

During the field research, while highlighting the progress that has been made in regard to the development of strategies and improvements in legislative harmonisation, respondents consistently asserted that progress has not been consistent in all areas. The top areas presenting challenges identified in the field research were progress in the area of (i) CSIRTS, (ii) incident reporting, (iii) investigations and procedures, (iv) public-private relationships, and (v) education. These will be discussed in the next section, but before that the report looks briefly at the government agencies working in this area, and highlights the challenges faced by them.

3.3.1 Government Agencies

A range of government agencies were identified as having some remit within the field of cyber and information security, such as national CIRTs, police, prosecutors, judges, training providers, and other support services, such as IT forensics services. Within economies, cooperation across these agencies is reportedly positive, especially at the operational and investigative levels. Three common and interrelated implementation challenges nevertheless emerged with respect to all of these agencies. These were lack of financial investment commensurate with the activities expected within economies' cyber security strategies; lack of sufficient staffing, in terms of both staff numbers and expertise[83]; and insufficient technological capacity to conduct their activities. Such criticisms were very prevalent in relation to law enforcement and prosecutorial responses in relation to cyber. Challenges still exist, despite the establishment of dedicated units to investigate cybercrimes in the majority of the WB6 economies. Many of these units are insufficiently staffed, and financially and technologically under-resourced, hindering them in their ability to do their job. For example, despite the presence of a dedicated unit to investigate cybercrimes and attacks in Montenegro, the unit is currently not resourced in the manner necessary for it to conduct its activities as designed.[84] Such limitations are evident in the unit's staff numbers, staff qualifications, and in respect to hardware and software infrastructure.[85] Accessing suitable staff has been hindered by lack of qualified staff within the police, unfavourable conditions within the unit at present, and the inability to recruit from outside. As a result, the substantive investigation level was described to us as not as it should be.[86] These are similar findings to ENISA which found that "skills and capabilities are the main concerns for organisations. The need for related training programmes and educational curricula remains almost unanswered".[87]

Criticism in relation to judges and prosecutors was different. The biggest criticism was the lack of sufficient knowledge in this area, coupled with complaints that because the number of cases with a cyber component is low, neither prosecutors nor judges get consistent experience dealing with them. For example, a dedicated cybercrime unit was established in the Albanian Prosecutor General's Office in 2014 and now deals with the majority of cases that contain a cyber element. While the unit works effectively, it was suggested that both prosecutors and judges need more training in this area, as experience in this area is limited amongst many. It was highlighted that this training should also include elements around safeguarding the rights of suspects and rights to privacy. Specifically, this could include instruction on how to conduct focused searches and investigations into IT systems.

Such accounts contribute to assertions that real progress has yet to be achieved by police, prosecu-

83 RB12 interviewed between 11 June and 21 June 2018 in Sarajevo, BiH.

84 RB23 interviewed between 17 and 19 June 2018 in Podgorica, Montenegro.

85 RB23 interviewed between 17 and 19 June 2018 in Podgorica, Montenegro.

86 RB23 interviewed between 17 and 19 June 2018 in Podgorica, Montenegro.

87 ENISA (2018). *ENISA Threat Landscape Report 2017*, p.7.

tors, and judges professionally tasked with securing WB6 cyberspaces. This lack of investment, staffing, and technological support appears to be in direct conflict with the NIS. The Directive states that "Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks".[88] It is acknowledged that many of these agencies and units nonetheless function well above the standards commensurate with their currently available resources. Similar criticisms have also been made in relation to CSIRTs.

3.3.2 Computer Security Incident Response Teams (CSIRTs)

The functions of all the CSIRTs in the WB6 are very similar, which is unsurprising given that they have all been largely structured in line with ENISA guidelines.[89] However, more pertinently, the CSIRT's levels of functionality are not consistent across all economies. With the exception of Bosnia and Herzegovina, all of the WB6 in accordance with the NIS have functioning national CSIRTs. As regards Bosnia and Herzegovina, the CSIRT was established in 2017 based on a Council of Ministers Decision. It is situated in the Bosnia and Herzegovina Ministry of Security, but it has not yet been resourced effectively and is still very much under construction, requiring resourcing in terms of staff, technology, and training. That said, the Albanian and Serbian CSIRTs are also limited in respect to their functionality. Both have staffing issues and are therefore limited in what they can achieve. The Albanian national CSIRT is in the procedural and practice development stage and others, like that of The Former Yugoslav Republic of Macedonia, are in the active stage. Progress is largely dependent on when the CSIRTs were established (see Table 1). For example, while both the Albanian and the CSIRT from The Former Yugoslav Republic of Macedonia are very proactive, building a solid foundation for the future, the latter CSIRT is just slightly further ahead in its journey. The approach of both of these CSIRTs is in line with ENISA's recommendations, which suggest a three phase growth path. The first year is for the unit to reach the basic step, intermediate two years later, and to be certifiable a further two years on. Using this three tired system is important as, the basic step is "the minimum for successful cooperation between teams on incident handling, the higher steps are needed to allow the members of the CSIRTs network to interact on all steps, including pro-actively, thus truly giving meaning to the word CSIRTs network".[90] Representatives from the CSIRTs interviewed, in Albania, Serbia, and The Former Yugoslav Republic of Macedonia, were quick to acknowledge their successes, but all recognised they had a lot more to do. They blamed this gap on similar issues to those already mentioned, deficient financing, under staffing, and technology deficits, coupled with a lack of awareness on the part of politicians of the risk of insufficient cyberspace security capacity.

None of the national CSIRTs in the WB6 are standalone agencies, but their positioning within governments is different across the region. The national CSIRT in Serbia is, for example, positioned within the Republic Agency for Electronic Communications and Postal Services (RATEL), the one in The Former Yugoslav Republic of Macedonia is in the Agency for Electronic Communications, and Bosnia and Herzegovina's national CSIRT is in the Ministry of Security. Critics noted the potential for a conflict of interest in cases where CSIRTs are situated in regulatory bodies. ENISA also encourages sectorial CSIRTs, displays 17 sectors or constituency CSIRT types on its website.[91] The existence and number of these sectoral CSIRTs (e.g. finance, telecommunications, energy, etc.) is not consistent across the WB6. This is a developing area however and all economies are likely to undertake increased activity in this regard over the next 18 months to two years, as they progress into the second and third phases of their development. Some sectoral CSIRTs nonetheless already exist. For example, there are academic CSIRTs in both Serbia and The Former Yugoslav Republic of Macedonia, situated in the Academic Network (AMRES)[92] and the National Academic and Research Network (MARnet) respectively.

One of the tasks of national CSIRTs is to monitor cyber incidents at a national level. The information gathered, coupled with other relevant and available information – possibly information already circulated within the CSIRT network – should then be used to enable CSIRTs to provide early warning, alerts, and announcements to relevant stakeholders about risks and incidents. According to ENISA, CSIRTs should also be tasked with responding to incidents and providing dynamic risk and incident analysis and situational awareness. To enable them to do this, the NIS states that "security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported".[93] However, representatives from the three CSIRTs interviewed noted that private sector companies are reluctant to report incidents despite obligations in law to do so. This is made more difficult given that such reporting obligations do not come with mandatory standards for cyber security infrastructure across all sectors in the WB6. However, this is not the case in all sectors. For example, in Bosnia and Herzegovina and Montenegro it is mandatory for the financial sector to have security protocols in place, while in The Former Yugoslav Republic of Macedonia, the telecommunications sector must do so. However, even in these cases, reporting is very low.

Interviewees described the rationale for non-reporting as threefold. First, companies fear reputational damage if they report attacks, with a major concern that reports will be leaked to the media. Second, there was a lack of confidence that law enforcement are properly equipped to conduct investigations and prosecutions in this area, with reporting therefore viewed as a waste of time. Third, a number of respondents noted that many companies do not have the capacity to identify when then have been attacked, thereby making it impossible to report.[94] This is not unique to the WB6, the EU Cyber Security Strategy notes that the private sector "still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture or to invest in security solutions".[95] A common refrain amongst cyber security practitioners is that until penalties for non-reporting are substantial enough, reporting will not happen.[96] However, penalties alone may not be enough, one cannot report something one does not know about. [97]

The EU's General Data Protection Regulation (GDPR), which entered into force on 25 May 2018, may provide a useful framework in this respect though. Under the GDPR, companies must comply with stringent data protection and privacy rules and be able to demonstrate their compliance with same. Fines for non-compliance are such that they make it a costly mistake for all sizes of business.[98] Others are sceptical that this will make any real difference however, reporting an overall lack of trust between the public and private sectors. On the other hand, this appears to be changing somewhat, with examples of informal networks emerging to share experiences, knowledge, and challenges faced by those charged with cyber security across the board. As mentioned above, the informal IT network that exists in Belgrade, Serbia was highly regarded. In The Former Yugoslav Republic of Macedonia the national CSIRT is also trying to develop such a network in order to foster an environment where organisations and individuals are willing to share even some information about cyber incidents.

3.3.3 Public Private Relationship Building

There is clear recognition of the need for better relationships between the public and private sector in the cyber security field. For example, in Bosnia and Herzegovina a group of ICT companies, Bit Alliance, in conjunction with the government and Ministry of Education, have developed a university course in software development, which came on stream in September 2018. Such progress has yet to translate into public-private partnerships (PPP) in this area, which are often seen as a quicker and more cost-effective means to deliver everything from policy to infrastructure than can be achieved by the public sector alone. Some reasons offered for this included the lack of tradition of PPPs in the region; the lack of demand for these type of initiatives; and the lack of recognition by governments of ICT experts from within WB6 economies and the preference, in many cases, for international experts.[99]

Certainly, the technical capacity to develop and grow PPPs is present within most WB6 economies. Our field research identified a number of IT and cyber security companies active locally and regionally, but also successfully doing business in Europe and even globally, thereby indicating they meet world-class standards. In fact, one important finding of the research is that the WB6 has a very dynamic and growing ICT sector that, if leveraged effectively, is likely to be a considerable asset to developments in this area now and into

88 Council Directive 2016/1148/EU Concerning Measures for a High Common Level of Security of Network and Information Systems, p.6.

89 The requirements of a national CSIRT are set out in Annex 1 of the NIS.

90 ENISA (2017). *Study on CSIRT Maturity: Evaluation Process*, Heraklion, Greece: ENISA, p.6: *https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process*.

91 See 'CSIRTs by Country - Interactive Map' on ENISA's website: *https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map*.

92 See the 'Institutions' page of the official AMRES website: *https://www.amres.ac.rs/en/institutions/csirt*.

93 Council Directive 2016/1148/EU Concerning Measures for a High Common Level of Security of Network and Information Systems, p.6.

94 RB11, RB12, R14 interviewed between 11 June and 21 June 2018 in Sarajevo, BiH.

95 European Commission (2013). *Cyber Security Strategy of the European Union*, p.6.

96 RB14 and RB24 interviewed in June 2018 in Sarajevo, BiH and Podgorica, Montenegro.

97 Article 21 of the NIS Directive places the onus on Member States to set rules on penalties applicable to infringements of national provisions adopted pursuant to the Directive. See Council Directive 2016/1148/EU Concerning Measures for a High Common Level of Security of Network and Information Systems, pp.'s 24.

98 They are scalable, ranging from €10 million or 2% of a firm's global revenue to €20 million or 4% of revenue, whichever is higher. See *https://www.gdpreu.org/compliance/fines-and-penalties/*

99 RB24 interviewed between 17 and 19 June 2018 in Podgorica, Montenegro.

the future. Furthermore, these ICT companies appear to be willing to implement stringent protocols and practices when required. For example, a number of private companies and business associations interviewed reported compliance with the GDPR, despite it not being a requirement to do business in the WB6.

A strategic objective of the EU's Cyber Security Strategy is promotion of EU core values, which includes preservation of an "open, free and secure cyberspace" that is acknowledged as "a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society".[100] WB6 economies are engaged with this aspect of the EU strategy to differing degrees. Positive examples of local, regional, and international cooperation are evident at the operational level, in the work of the Belgrade Security Forum (BSF), DCAF, and the Regional Cooperation Council (RCC). For example, DCAF conducted a project to enhance good cyber governance with cyber security experts in Serbia and other Western Balkan economies, one aspect of which was to review methods to make governments' online services more secure.[101]

As of 1 July 2018, DCAF has also begun a three-year regional project entitled "Enhancing Cybersecurity Governance in the Western Balkans" (2018-2021), which is funded by the UK Foreign and Commonwealth Office's Cyber Security Fund, and focused on Bosnia and Herzegovina, The Former Yugoslav Republic of Macedonia, Montenegro, and Serbia. The project has three main objectives: (i) raising awareness of decision-makers from all Western Balkan economies on the need to cooperate regionally and internationally, by bringing senior cyber security actors from the public and private sectors together at high-level regional cyber security conferences; (ii) supporting better cyber security coordination at the national level in Bosnia and Herzegovina, The Former Yugoslav Republic of Macedonia, Montenegro, and Serbia by supporting the organisation of annual national multi-stakeholder roundtables in each of the four economies; and (iii) strengthening the capacity of national/governmental CSIRTs in the Western Balkans to respond effectively to incidents and encouraging regional and international cooperation through Western Balkan CSIRT staff's participation in international cyber drills and conferences, as well as joint trainings. UK support in this area is likely to continue with a recent announcement of a £1m investment in training and advisory activities for cyber security in the region.[102] Problems nevertheless exist in this realm also. Similar to other areas, donors do not always coordinate and there can be considerable overlap in activities. That said, there is growing recognition of this, as many of the organisations working in this area, at least at the regional level, are trying to be more strategic.

Not in question in our field research was recognition and awareness across the WB6 that cooperation at all levels is key in the cyber security area. Respondents mentioned the need for greater cooperation because cyber criminals rarely respect traditional jurisdictional boundaries and therefore joint investigations are common. Some highlighted that lack of technical capabilities resulted in receiving support from others in the region. It was noted that cooperation often moved beyond this to problem-solving, with the ability to ask others with experience of similar issues described as "priceless". The importance of this was even more relevant at the regional level. Interviewees uniformly acknowledged more needs to be done both at the national and regional levels and while many noted that whilst differences exist within the region, most WB6 economies face similar challenges and therefore solutions are likely to be similar. Regional cooperation was therefore justified as imperative to progress. Furthermore, many of the economies share similar legislative structures, which should enable shared learning and problem solving. All WB6 economies are, in addition, moving towards accession to the EU, and therefore face a shared route on this journey, and a common future goal. It was acknowledged too that the WB6 are all positioned relatively similarly in relation to cyber security so can share experiences, challenges, and successes along the way. Progress can be achieved in economies that want to move forward, which can then act as influencers for the others.

3.3.4 Civil Society

The EU also notes the need for Member States to work with civil society in relation to preserving an open, free, and secure cyberspace. However, such relationships between the WB6 economies were found to be somewhat limited. Many civil society organisations (CSOs) are dependent on the donor community for resources and, as a result, their work is largely driven by donor requirements. The priority for the donor community in the WB6 is post-conflict issues that have, for the most part, not been related to cyber security. There is thus a lack of oversight of cyber security and related issues by CSOs in the WB6, despite recognition of its importance, especially as regards human rights and privacy. Concerns were expressed about this during our field research. Some feared that without civil society, wide ranging surveillance and censorship could be introduced.[103] Many interviewees raised the need to support increased CSO activity in the cyber security field, broadly defined, to monitor and oversee government activity.[104] That said, CSOs are more active around cyber security-related issues at the regional level, which is evident by the new UK-funded DCAF project referred to above. It was reported however that it can be difficult to implement or translate regional cyber security programmes to the national level due to the lack of local CSOs tasked in the area.

3.3.5 Education

Under the EU Cyber Security Strategy's objective of 'achieving cyber resilience', Member States are invited to:

> [S]tep up national efforts on NIS education and training, by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations.[105]

Similarly, the importance of education and training in the area of ICT was identified as a key component to good information security in WB6. So too was the need for a more multi-disciplinary approach to education in this sector. One that includes not just technical aspects of ICT and information security, but also courses on relevant legislation, regulation, policy development, strategic management of the ICT sector, implementation management, etc. Such courses are necessary to ensure people are equipped with the necessary skills to translate the technical aspects of ICT and related security into appropriate policy and practice. The Masters level programme in the University of Donja Gorica, Podgorica, Montenegro was the only programme in the region identified as offering such training albeit programmes in the University of Pristina and American University in Sarajevo were identified as providing courses in the broader areas of information and cyber security. The existence of these courses notwithstanding, there is an apparent lack of educational policies focusing on ICT and related security in the WB6.

A number of interviewees across the WB6 stated that they did not think that current third level structures were producing sufficient numbers of qualified graduates for the cyber security sector. Many operational experts, both public and private, reported the lack of a long-term vision within the WB6 and their relevant education sectors about the current numbers being trained in comparison with future requirements within this sector. The same interviewees highlighted that this lack of strategic thinking will have a significant long-term impact if not addressed. Also acknowledged was that universities often lack funding to install the necessary technological infrastructure, such as ICT laboratories; attract relevant experts; and engage in ongoing research and development. These all influence the nature and quality of the courses being offered. Some reported that there is also a deficiency in much of the education sector in respect to market needs. This was illustrated by a range of private sector companies and related associations that reported the need to further enhance the skills of graduates after university to ensure they were capable of performing at the level required on taking up employment in the sector. This has resulted in an increasing range of private training courses being made available. Some of these are delivered online from within the region, others are accessing such training online via international vendors. That said, it was also highlighted that formal third level education is not and should not be the only route into this sector. Many skilled cyber security practitioners acquire their skills 'by doing', more specifically by honing their skills in the very activities they later learn to defend against. This is a reality that is unlikely to change, but can be supported through further training, accreditation, licencing, registration, etc.

Many respondents also highlighted the lack of or limited education in the field of information security in primary and secondary schooling. They noted that more targeted learning should be provided at these education levels. For example, how to use certain software and systems, some basic programming, knowledge about operating systems, guidance on source checking, how phishing works, how to use encryption, and similar. This would ensure future generations are aware of both the benefits and threats associated with online systems. While examples of awareness raising campaigns exist across the WB6, it is recognised that awareness of basic cyber security is not at the level that it should be. One positive example of where such education has been formally entered into the curriculum is in Albania, where the national CSIRT has worked

100 European Commission (2013). *Cyber Security Strategy of the European Union*, p.14.

101 DCAF (2017). *DCAF Annual Report 2017*, Geneva: DCAF, p.19: *https://www.dcaf.ch/sites/default/files/imce/About-Dcaf/DCAF%20Annual%20report%202017_AW.pdf*.

102 European Western Balkans (2018). 'UK's Doubled Financial Package for Western Balkans Aimed Mainly towards Security Challenges', 10 July: *https://europeanwesternbalkans.com/2018/07/10/uks-doubled-financial-package-western-balkans-aimed-mainly-towards-security-challenges/*.

103 RB20 interviewed between 13 and 16 June 2018 in Belgrade, Serbia.

104 RB20 interviewed between 13 and 16 June 2018 in Belgrade, Serbia.

105 European Commission (2013). *Cyber Security Strategy of the European Union*, p.8.

with the education sector to ensure its inclusion. Other examples of progress also exist. For example, in Bosnia and Herzegovina, the private sector has started providing coding courses to students throughout the country via the global Coder Dojo network of free computer programming clubs for young people, which is being very well received. While it is clear that the WB6's education sector is somewhat deficient in terms of cyber security, such examples show the benefits of both public and private sector activities in this field.

3.3.6 Media

Interestingly, the EU's Cyber Security Strategy does not specifically mention the media. However, during our research, the role of media was identified as important, but informed reporting on cyber security and related issues was noted as lacking in the majority of the WB6.[106] Where such topics are covered, media articles and commentary were said to have little substance, often simply focusing on the role of Russia rather than investigating more deeply. Highlighted was not only the lack of awareness amongst many journalists of the increasing importance of covering cyber and information security issues, but also, despite the provision of training by international and regional organisations, how to be in safe online contact with sources and the protection of both journalists and their sources' cyber security.[107] Interestingly, it was acknowledged by journalists that many sources have a greater awareness of the need to maintain their own security and are moving to more secure communication options.[108]

3.3.7 Other challenges

One key concern across all respondents related to 'brain drain'. All WB6 economies reported high rates of migration in general, but also in respect to ICT professionals. Many interviewees reported significant concerns that the majority of ICT professionals that are leaving are those with 10+ years of experience, thereby significantly draining the level of expertise available in the cyber security sector. It was also noted that despite progress at the legislative level, a recognition that more needs to be done in this area to harmonise with the EU framework, and an awareness of existing challenges and obstacles, many still fail to see cyber security from a risk management perspective.[109] This was a criticism not just levelled at governments, but also at the private sector. It was suggested that IT systems are not robust in the same way physical structures are, in that service providers are not held to account if problems occur. For example, engineers building a bridge need to ensure certification to the highest standards. They need to have the proper training to work on it, have the proper insurance, etc. This is not always the case in respect to IT engineers. It was argued that the same incentives are not there to motivate action in this area by clients or by service providers. Even where clients do take action where quality is in question, IT companies are rarely held accountable if something goes wrong with their software or hardware.[110]

Many respondents noted that cyber security will only be taken seriously when attacks become more prevalent and impactful. It was claimed that for the most part neither governments nor companies within the WB6 are high value targets for such attacks, but this may change as advancements in ICT continue. Another very important challenge identified consistently across the WB6 related to an apparent lack of awareness of cyber security risks. Interestingly, this was attributed to all, from citizens right up to the government. As a result, many noted that awareness raising was a key necessity in parallel with legislative and operational change in this area. Interestingly, it was suggested that there is also a lack of understanding and awareness at the donor level.[111]

3.3.8 Funding

Very little documentation could be located on how the WB6 fund or intend to fund their cyber security commitments, either at regional or economy level. While donor funds are available as mentioned above, progress cannot be funded on donor investment alone.

This section has illustrated many of the challenges and obstacles that still remain in respect to the successful implementation of activities in the area of cyber security in the WB6. At the same time, it is evident that progress is being made and although deficiencies do exist, the majority of those we spoke to during our field research appeared to be eager, committed, and highly qualified. If their energy and commitment can be leveraged, supported by the necessary investment, significant future progress is not in doubt.

106 RB10 interviewed between 11 and 12 June in Sarajevo, BiH.

107 RB10 interviewed between 11 and 12 June in Sarajevo, BiH.

108 RB25 interviewed between 17 and 19 June 2018 in Podgorica, Montenegro.

109 RB27 interviewed between 17 and 19 June 2018 in Podgorica, Montenegro.

110 RB12 interviewed between 11 and 21 June 2018 in Sarajevo, BiH.

111 RB26 interviewed between 17 and 19 June 2018 in Podgorica, Montenegro.

4. MINI ECONOMY CASE STUDIES

This section provides mini case studies on each of the WB6 economies. Its purpose is to provide insight into the progress of each economy in the area of cyber security, discuss key actors involved, and some of the key challenges, whilst identifying some positive examples of progress.

4.1 Albania

As of 2017, approximately 2 million people or 66% of Albania's population were internet users.[112] This grew from .1% of the population in 2000. [113] People are moving away from fixed-line telephony to mobile solutions, with only approximately 30% of households now having fixed line connections and mobile internet penetration at around 80%. While this has helped support government efforts to roll out e-government services, there is a significant gap in access between urban and rural areas. Rural areas represent 40% of the population, but only 1% are connected to the internet.

4.1.1 Cyber Security Strategy

Albania does not have a Cyber Security Strategy *per se*, the Paper on Cyber Security 2015 – 2017 suffices in its absence. The purpose of the Policy Paper was "to review and coordinate the obligations that stem from the commitments that are undertaken for a safe cyberspace, in order to ensure fulfilment of responsibilities of all actors in a coordinated way".[114] It draws on a number of existing strategies and policies, including the National Security Strategy 2014 – 2020, the Digital Agenda for Albania 2014 – 2020, which is in line with both the Digital Agenda for Europe 2020 and the EU Cyber Security Strategy. Albania ratified the Budapest Convention in June 2002. Complying with Article 35 of the Convention, the government appointed a 24/7 contact point, within the Cybercrime Unit of the Albanian State Police. Cooperation is good, but it is not used as well as it could be.

From an investigative perspective, many interviewees reported very good relationships with the FBI, Interpol, Europol, and other states' police agencies, albeit both police and prosecutors highlighted that some are less willing to cooperate than others.[115] Furthermore, it was acknowledged that cooperation is resources intensive, so it is often reserved for serious cases.[116] Locally, good cooperation is reported with Serbia and Kosovo*, but it is mostly

112 Internet World Stats (2017). 'Europe'.

113 Internet Live Stats (2018). 'Internet Users'.

114 Republic of Albania (2015). *Policy Paper on Cyber Security 2015-2017*, Tirana, p.9: *http://ncsi.ega.ee/app/uploads/2016/05/Policy-Paper-on-Cyber-Security-2015-2017-Eng.doc*

115 RB5 interviewed between 30 May and 2 June 2018 in Tirana, Albania.

116 RB6 interviewed between 30 May and 2 June 2018 in Tirana, Albania.

at a basic level.[117] Training has been provided by international organisations. For example, the OSCE has conducted a number of activities relating to cyber security and disaster management, focusing on critical infrastructure, an area that was highlighted as requiring further training.[118]

4.1.2 Government Agencies

The key bodies with responsibility and competence in the area of cyber security include the National Agency for Information Society (AKSHI), the National Authority for Electronic Certification and Cyber Security (AKCESK), the Albanian State Police, and the General Prosecutor's Office. AKSHI was established in 2007. Its main aim is to act as the specialist agency on e-government and information society in Albania. E-government services first became available in 2008 and have been rolled out further since.[119] AKSHI ensures "safe authentication and identification, safe internet and DNS for the public administration in the services that it provides at the Government Data Centre".[120] It also has responsibility for electronic information, websites, and data centres of the majority of government ministries. A single data centre ensures all information is centrally protected.[121] This approach while cost-effective and logical in many respects, is a single point of failure, if attacked.

In 2017, the Albanian National Agency for Cyber Security (ALCIRT) and the National Authority for Electronic Certification (NAEC) merged to create AKCESK. AKCESK's main activities relate to the "supervision and enforcement of legislation in the field of electronic signature, electronic identification of trusted services, as well as enforcement of legislation in the field of cyber security".[122] The National CSIRT is situated in AKCESK and has a legal requirement to investigate cases of cybercrime against the state, but at present does not have the capacity to do so. Since its establishment, the Authority has been developing its methodology and procedural framework and has conducted considerable work in regards to awareness raising. The latter has included running a Cyber Academy for university students, where private companies also came to interact with students. The Authority also holds an annual internet safety day at secondary schools to highlight the risks of cyber space for second-level students. They have also been successful in getting ICT included in the education curriculum of grade 6 and 7 students throughout Albania. AKCESK is also currently drafting an ICT policy and is providing political and technical support to government authorities in this area. While it is acknowledged that a lot has been achieved within the first year of establishment, AKCESK wants to quickly get to a stage where it is fully functioning.[123]

The Albanian State Police is responsible for investigating any reported crimes related to cyber security. In 2009, a dedicated cybercrime unit was established in the Albanian State Police. This unit is reportedly well structured, trained to a good standard, and competent. The State Police has established an internet site where citizens can report, in real time, any criminal act related to cybercrime. A dedicated cybercrime unit was also established in the General Prosecutor's Office in 2014. This unit deals with the majority of cases that contain a cyber element. It was suggested that both prosecutors and judges need more training in the cyber area, including training on how to conduct focused searches and investigations into IT systems, but also around safeguarding the rights of suspects and the right to privacy.

4.1.3 Incident Reporting

Cybercrime offences are enshrined in the Criminal Code of Albania and the Electronic Communication Law. As the internet penetration rate increased so too did the number of violations of computer networks in Albania.[124] The majority of cybercrime cases relate to fraud; other cases include hacking, online stalking, and data interference. Hacking cases often involve nationals and internationals, while online stalking cases largely involve nationals, as do data interference cases.[125] The number of registered criminal proceedings related to computer fraud has increased, but convictions still remain low: five in 2017, against one in 2016, and four in 2015.[126] It was asserted that the government experiences between five and 10 cyber attacks per year, with about six being problematic.[127] The majority of these have been Denial of Service (DoS)-type attacks.[128]

4.1.4 Relationships between Public and Private Sector

Relationships with Albania's private sector are not at the level that they should be. For example, it can be difficult to get information from some internet service providers (ISPs) without a court order and as the formal relationship for investigating cybercrime is between the ISP and prosecutors, it can be difficult for the police to be proactive in this area. A specific area identified where improvement is needed within the private sector relates to internet protocols (IPs): more work needs to be conducted with telecom companies to develop technologies in order to better manage, understand, and monitor IP addresses. It was also suggested that Albania needs to adopt IPv6, as it is currently using IPv4.

Academic progress in the ICT sector has not kept pace with the speed of ICT development and the market suffers as a result. There are few, if any, master's degree programmes in information or cyber security in Albania. This has a direct impact on the private sector, which often finds it difficult to hire adequately qualified people.[129] Investment in ICT in schools has also been limited. IT labs are not up to today's standards in most schools.[130] Furthermore, there is little civil society activism in the area of cyber security in Albania, except in the area of youth and the risks posed to them while online.[131] This is due to a number of factors, including the difficulty of attracting technical experts to CSO work. Without the latter it can be difficult to translate technical needs into policy recommendations, which impacts the ability to lobby.[132] Another reason for low levels of CSO involvement is the lack of donor investment in this area. State investment in civil society is also low, and therefore, CSOs are often reliant on international donors and addressing their priority areas.[133]

4.1.5 Assessment

Albania is well-prepared as regards legislation generally, and the area of cyber security is no different. This was reaffirmed by the EU which found in its 2018 assessment that the Law on Cyber Security is partly aligned with the NIS, further noting Albania is moderately prepared in the area of information security, highlighting progress in relation to the digital agenda action plan, e-government services, the cross-sectoral strategy of Albania's digital agenda for 2015 – 2020, and the plan for broadband development. The EU assessors also mentioned good progress in the area of electronic communications with approval of the law on development of high-speed electronic communication networks, stating that this law fully complies with the *acquis*. However, obstacles and challenges hindering institutional capacity within government authorities remain, including as regards staffing, training, and technical capacity.[134] Relationships between the public and private sectors need to be harnessed better in this area.

4.2 Bosnia and Herzegovina

A little under 3 million or 80% of BiH's population are internet users.[135] This grew from 1.1% of the population in 2000.[136] The citizens of Bosnia and Herzegovina now have access to similar ICT technologies and opportunities available elsewhere in Europe.[137] That said, the same pace of advancement has not been kept with respect to cyber and information security in Bosnia and Herzegovina at the government level. Legislation has not been fully harmonised and implementation of e-government has been slow.[138]

4.2.1 Cyber Security Strategy

Bosnia and Herzegovina lacks a state level strategy addressing cybercrime and cyber security threats, which has hindered the level of progress at the state level. That said, the Council of Ministers of Bosnia and Herzegovina adopted the Strategy for establishment of a CSIRT in Bosnia and Herzegovina in 2011 and adopted the Decision on Establishment of Computer Emergency Response in March 2017. Furthermore, issues with regard to cybercrime and cyberterrorism are mentioned in the Strategy for

117 RB6 interviewed between 30 May and 2 June 2018 in Tirana, Albania.

118 RB1, RB2, RB5, and RB6 interviewed between 30 May and 2 June 2018 in Tirana, Albania.

119 Five hundred and seventy one electronic services are said to be provided on the e-government portal; see *http://akshi.gov.al/*.

120 Bahiti, R. and Joshi, J. 2015. 'Towards a more resilient cyberspace: the case of Albania', *Information and Security An International Journal*, vol.32, 2015, p.6.

121 There are 420 websites hosted through the data centre. See *http://akshi.gov.al/*.

122 From AKCESK's official website: *http://www.akce.gov.al/index.html*.

123 RB2 interviewed between 30 May and 2 June 2018 in Tirana, Albania.

124 Bahiti, R. and Joshi, J. 2015. 'Towards a more resilient cyberspace: the case of Albania', *Information and Security An International Journal*, vol.32, 2015.

125 RB6 interviewed between 30 May and 2 June 2018 in Tirana

126 European Commission Staff (2018). *Albania 2018 Report*, p.35.

127 RB2 interviewed between 30 May and 2 June 2018 in Tirana

128 RB2, RB4, and RB5 interviewed between 30 May and 2 June 2018 in Tirana

129 RB3 interviewed between 30 May and 2 June 2018 in Tirana

130 RB3 interviewed between 30 May and 2 June 2018 in Tirana.

131 RB7 interviewed between 30 May and 2 June 2018 in Tirana

132 RB8 interviewed between 30 May and 2 June 2018 in Tirana

133 RB7 and RB8 interviewed between 30 May and 2 June 2018 in Tirana

134 RB2, RB5, and RB6 interviewed between 30 May and 2 June 2018 in Tirana

135 Internet World Stats (2018). 'Internet in Europe Stats': *https://www.internetworldstats.com/stats4.htm*.

136 Internet World Stats (2018). 'Bosnia-Herzegovina: Internet Usage Stats and Telecom Reports': *https://www.internetworldstats.com/euro/ba.htm*.

137 Barakovic, S. and Barakovic Husic, J. (2015). 'We Have Problems for Solutions: The State of Cyber Security in Bosnia and Herzegovina,' *Information & Security: An International Journal*, 32(5).

138 RB11 interviewed between 11 and 21 June 2018 in Sarajevo

Fighting Organised Crime (2014-2016) and in the Strategy for Prevention and Fight against Terrorism (2015-2020). Additionally, the BiH authorities ratified the Budapest Convention in March 2006 and appointed a 24/7 contact point, within the Directorate for Coordination of Police Bodies of Bosnia and Herzegovina. Cooperation within the region and internationally is reportedly good. However, the lack of a state level strategy can make this difficult.[139] An area of cooperation highlighted that needs to be enhanced relates to cyber exercises. It was reported that such activities are excellent and a really valuable learning opportunity.[140] Support provided by the international community, in the form of training, workshops, and education and additional training was therefore described as always welcome.[141]

4.2.2 Government Agencies

The Ministry of Security houses the national CSIRT.[142] Its mandate includes services relating to the provision of information on potential vulnerabilities and management of incidents in the domain of electronic security to all state level institutions and their supporting service providers. While it exists on paper, it has not yet been adequately resourced however.[143] The Republic of Srpska (RS), as one of two entities within Bosnia and Hercegovina, established the Department for Information Security which is situated in the Agency for Information Society. This is tasked with coordination, prevention, and protection from incidents, as well as supervision of the implementation of measures and standards related to information security in the RS. This functions as the CSIRT at the entity level and has been operational since 2015.

In respect to policing, specialised cybercrime units were created within the Federation of Bosnia and Herzegovina Police Administration and in the Ministry of Interior to deal with cybercrime. In Brčko District cybercrime is investigated by specialised investigators in the police. Nonetheless, challenges exist. For one, despite dedicated units, the majority are modest, despite in many cases being staffed by eager and willing personnel.[144] They are small in number and many do not have the technical capacity to deal with the challenges of existing and emerging cyber threats.[145] Digital forensics is carried out by the State Investigation and Protection Agency (SIPA), Border Police of Bosnia and Herzegovina, Agency for Forensics and Expert Examinations, the Ministry of Interior of Republka Srpska, Brčko District Police, and cantons' Ministries of Interior.[146] Prosecutors dealing with serious organised crime usually process cyber cases. Because the criminal code is largely the area of competency at the entity level, prosecutors at this level deal with the majority of these cases.

4.2.3 Incidents

The main types of cybercrime in Bosnia and Herzegovina include DoS and DDos attacks, internet fraud, unauthorised access to computer systems, credit card scams, wireless network abuse, online child sex abuse-related activity, online intellectual property rights violations, social network abuse, distribution of malware, inciting hatred, discord or intolerance, and public incitement to terrorism and terrorist propaganda. These offences are largely dealt with under the criminal code at the entity level. There are no meaningful statistics regarding cyber attacks on CII in Bosnia and Herzegovina. Attacks on government websites and cyber infrastructures have been reported, but are not believed to have been very serious to date.

4.2.4 Relationships between Public and Private Sector

Relationships between the private sector and government are limited with regard to cyber and information security in Bosnia and Herzegovina. However, private sector ICT companies are trying to work with the government to improve this situation as both sides recognise the benefits of working together. For example, private sector ICT companies have worked with the government in the area of child safety. Another public-private sector partnership resulted in the development of a new two-year academic software development course, which will help meet the needs of the market.[147] The banking sector is also very progressive in the cyber security area, largely because of strict legally mandated obligations.[148] It is the only sector that is legally obliged to have cyber security systems in place,[149] and must also have dedicated CIS officers and conduct regular audits.[150] These obligations have resulted in the growth of companies and businesses offering cyber security expertise. As a result, good technical competency within the private sector is evident in Bosnia and Herzegovina, which is being actively deployed both at home and internationally.[151]

In respect to academia, access to ICT related education is not at the level required, but there is progress.[152] Some proactive professors are introducing new courses and inviting expert guest lecturers to broaden the curriculum. The private education sector is also attempting to bridge the gap. For example, the American University has developed the South-East Cyber Security Centre, which offers cyber security training at both the Masters and PhD level. [153] Some private companies are also providing online training courses. However, despite this cooperation between the university and security, intelligence, and defence institutions, there appears to be little systematic alignment at the government level as regards future ICT requirements, in terms of manpower and educational courses being offered.[154] The same challenges exist at primary and secondary levels. There is no consistency in cyber education in schools. Some are well equipped, while others have little. However, positive examples do exists. The private sector is working to provide high school students with opportunities for them to take part in coding training.[155] These courses are conducted throughout the country and are very well received.[156]

In regard to civil society, there does not appear to be active civil society involvement in the area of cyber security in Bosnia and Herzegovina. Nonetheless, many recognise the need for greater effort in this area. Those with previous experience in the area reported that it is difficult to question the government about their activities around cyber security, which negatively impacts their work.[157] Interestingly, CSOs reported being the victims of cyber attacks. Some of these attacks were sophisticated to the point that they would have taken months to prepare and were most likely perpetrated for purposes of accessing specific pre-identified resources.[158] Similar to the private sector, many CSOs noted difficulties reporting cyber security incidents, saying that they would rather conduct post mortems themselves to learn about the nature of attacks in order to better understand how to prevent them in the future, rather than report them.[159]

4.2.5 Assessment

There is no culture of security information in Bosnia and Herzegovina as of yet. While there is a willingness to make improvements in the area, interviewees reported that government still lacks awareness and understanding of the potential impacts of cyber security issues.[160] The EU noted this in its 2018 assessment, observing that Bosnia and Herzegovina lacks a strategic framework to address the issue of cybercrime and cyber security threats and cybercrime investigations reportedly remain very rare. There is a perception that there is no imminent threat, and therefore does not require additional input at present. However, the State Investigation and Protection Agency (SIPA) is a noticeable exception at the state level. It identified the need for a cyber security strategy and proactively developed and adopted its own strategy and action plan. [161] This includes the development of a CIRT, which is currently in the planning phase.[162] The Ministry of Defence's (MoD) strategy was not designed to replace a state level strategy, rather designed to complement the state's strategy when it becomes available. Also, the MoD activity is not adequately resourced, but positive progress is being made. The lack of finances is not only evident within the MoD, interviewees noted that there has not been the necessary budgetary investment in this area at the state level from hardware, software, and staffing perspectives, yet it is difficult to achieve excellence without it.[163]

One positive that was mentioned that reduces the risk posed to the government from cyber attacks is that historically critical IT systems have not been integrated, thereby reducing the potential damage if attacked. However, that is now changing, which means increased risk.[164] The lack of investment in

139 RB17 interviewed between 11 and 21 June 2018 in Sarajevo

140 RB17 interviewed between 11 and 21 June 2018 in Sarajevo

141 RB15 interviewed between 11 and 21 June 2018 in Sarajevo

142 RB15 interviewed between 11 and 21 June 2018 in Sarajevo

143 RB14 and RB17 interviewed between 11 and 21 June 2018 in Sarajevo

144 RB11 interviewed between 11 and 21 June 2018 in Sarajevo

145 RB12 interviewed between 11 and 21 June 2018 in Sarajevo

146 RB15 interviewed between 11 and 21 June 2018 in Sarajevo

147 RB14 interviewed between 11 and 21 June 2018 in Sarajevo

148 RB11, R13, and RB15 interviewed between 11 and 21 June 2018 in Sarajevo

149 RB14 interviewed between 11 and 21 June 2018 in Sarajevo

150 *Ibid.*

151 RB13 interviewed between 11 and 21 June 2018 in Sarajevo

152 *Ibid.*

153 RB15 interviewed between 11 and 21 June 2018 in Sarajevo, BiH. See also Minovic, A. *et al* (2016). *Cyber Security in the Western Balkans*, p.17.

154 RB12 interviewed between 11 and 21 June 2018 in Sarajevo

155 RB12 interviewed between 11 and 21 June 2018 in Sarajevo

156 Rolling out programmes countrywide can be difficult from a technological perspective. Infrastructure is good in urban areas, but this is not consistent across the country and can hinder success.

157 RB11 interviewed between 11 and 21 June 2018 in Sarajevo

158 RB11, RB12 interviewed between 11 and 21 June 2018 in Sarajevo

159 RB11 interviewed between 11 and 21 June 2018 in Sarajevo

160 RB11, RB15, and RB16 interviewed between 11 and 21 June 2018 in Sarajevo

161 RB11 interviewed between 11 and 21 June 2018 in Sarajevo

162 RB17 interviewed between 11 and 21 June 2018 in Sarajevo

163 RB15 interviewed between 11 and 21 June 2018 in Sarajevo

164 RB17 interviewed between 11 and 21 June 2018 in Sarajevo

staff has a significant impact on accessing the necessary skill set within the public sector, as the private sector is currently driven by a growing market, which is a lot more competitive both at home and abroad.[165] Furthermore, there are concerns that the education systems are unlikely to produce trained personnel, in the numbers and areas of expertise required, for some time to come. The universities are not producing the calibre of graduates needed, resulting in many getting trained abroad, some self-learning, and companies having to offer on-the-job training.[166] While these are all viable options, it all requires considerable investment. Additionally, it is difficult to retain staff once they have gained experience because of the dynamics of the market, with many deciding to migrate further afield for work. [167]

4.3 Kosovo*

As of December 2017, the internet penetration rate in Kosovo* was 84%,[168] which is comparable with global norms. Kosovars were found to use the internet as much as European citizens, if not more. However, it is acknowledged that without a top level domain, businesses cannot link their corporate websites to the economy, which can be problematic for shopping online, for example.[169]

4.3.1 Cyber Security Strategy

In 2016, Kosovo* adopted a National Cyber Security Strategy and Action Plan 2016-2019. The strategy includes five strategic objectives to ensure a safe cyber environment, namely: critical information infrastructure protection; institutional development and capacity building; public and private partnership building; incident response; and international cooperation.[170] It also references respect for privacy, fundamental rights and liberties, free access to information, and democratic principles. For the most part, Kosovo* has very good legislation, and in many ways, the area of cyber security is no different, as was recognised by the EU, which noted in its 2018 assessment that Kosovo's* legislation on cybercrime is largely in line with the EU *acquis*.[171] While some revision to the legislation is needed, the biggest issue relates to implementation, which has not yet been done to the level required.

Additionally, in relation to information society, the EU's assessment report noted that adequate budgetary resources were required to enable the implementation of the cyber security strategy and action plan as envisaged. The Cyber Security Strategy states that international cooperation in this area is a priority for Kosovo.*[172] As a step towards achieving this, the government appointed a 24/7 contact point within the police's cybercrime unit. International cooperation is good, but it could be improved within the region.[173] It was recognised that cooperation could be enhanced by improving the ability to collect evidence in real time as delays negatively impact investigations. International organisations such as ICITAP, the EU, and OSCE were all identified as providers of support and training in this area.[174] Their input was deemed to be highly useful. It was recognised that the inability to participate in training provided by NATO and some EU trainings was a hindrance, especially given the recognition that such training was of an excellent standard.[175]

4.3.2 Government Agencies

The National Cyber Security Strategy includes an innovative element, which relates to the appointment of a National Cyber Security Coordinator. It was envisaged that this position would be held by the Minister of Internal Affairs or his/her deputy, and would be responsible for and mandated to coordinate, guide, monitor, and report on implementation of policies, activities, and actions in this area. The strategy also sets out the establishment of a National Cyber Security Council, which includes representatives from the private sector, the ultimate goal of which is to strengthen cooperation between the public and private sectors. The strategy itself was developed by a multi-disciplinary working group, led by the Ministry of Internal Affairs, including representatives from state institutions, professional associations, the private sector, civil society, and international partners.

Another important government agency in this area is the Agency for Information Society. It has the responsibility for coordination, management, and monitoring of processes and mechanisms of electronic government in relation to ICT infrastructures and expansion. A national CSIRT has been established within the Regulatory Authority for Electronic and Postal Communication, supported by other sector specific CSIRTs.[176] They all cooperate with each other, and all share the roll of improving awareness at their respective levels.[177] The main function of the CSIRTs is prevention of serious incidents relating to network and information security. The national CSIRT also plays a key role in safeguarding electronic communication networks and services and their users in Kosovo*.

In respect to policing, the competent authority is the Kosovo* Police. A Cybercrime Investigation Sector was established within the police in June 2011 and became operational in September 2011. It is situated in the Directorate for Organised Crime Investigation and reportedly receives specialised training and equipment.[178] It was nonetheless acknowledged within the National Cyber Security Strategy that improvements in professional education and training were needed for police specialists and others professionally tasked in this area. It has been suggested that this needs to take place in a multidisciplinary environment to enhance policing.[179] The police are supported by the Forensic Agency, which has a dedicated IT Forensic Department. The National Intelligence Agency also provides support in relation to cyber security, focusing largely on collecting information on people and/or groups that pose a threat to national security.

4.3.3 Incidents

As in other economies, it is difficult to get accurate or indicative statistics relating to either cybercrime or cyber attacks. This is made more challenging because many private sector organisations are not reporting cyber incidents.[180] However, this is slowly improving. Nonetheless, from what is known, the most common type of cybercrimes include credit card fraud, fake news (e.g. through forged e-mails to the media), computer intrusion, DDoS attacks, phishing, and related. According to data supplied in the National Cyber Security Strategy, the main targets of attack include individual user accounts, the banking system, and websites. Even where incidents are reported, it is hard to detect where crimes originate, never mind investigate them, because many happen from the outside of this economy. It was alleged that a high percentage of incidents are the result of human failure, so more awareness raising is needed at all levels of society, reinforced through formal and informal education, starting with children so everyone is aware of the risks and benefits of the internet.[181]

4.2.4 Relationships between Public and Private Sector

Despite a lack of tradition of PPPs in Kosovo*, good relations between the public and private sectors, especially in respect to ISPs, were reported. However, cooperation is still not where it could be, despite it being prioritised within the National Cyber Security Strategy.[182] It was asserted that even where private sector experts are needed by the government, the government has a tendency to use international experts rather than looking closer to home.[183] The government should be encouraged to work with local companies to build better responses in this area to harness such skills,[184] particularly because many local companies are already trading in this area internationally, which indicates they have the necessary expertise and meet necessary standards.[185]

On a positive note, the University of Pristina is providing quality educational programmes, with increasing numbers entering employment on finishing these degrees.[186] Their quality is also evidenced by the number of students winning awards nationally and internationally for their work.[187] It is acknowledged however that it can be difficult to access experienced academics in certain areas, which has an impact on the type of courses that can be offered. It is also difficult to conduct research in the area, as there are very little additional funds available. Ideally additional investment would be made to enable more hands-on training in laboratories and support further research, to ensure the IT education sector is producing qualified experts at the level and number needed within the sector.

Many students are finishing university with a basic grounding in ICT, but much of what they learn is outdated and does not meet market needs.[188] STIKK, an association of IT professionals, responded by designing a seven-month national programme, funded

165 RB14, RB15, and RB17 interviewed between 11 and 21 June 2018 in Sarajevo

166 RB16 interviewed between 11 and 21 June 2018 in Sarajevo

167 RB15 interviewed between 11 and 21 June 2018 in Sarajevo

168 Internet World Stats (2017). 'Europe'.

169 RB15 interviewed between 11 and 21 June 2018 in Sarajevo

170 Kosovo* (2015). *National Cyber Security Strategy and Action Plan 2016 - 2019*, Dec., Pristina: *http://www.kryeministri-ks.net/repository/docs/National_Cyber_Security_Strategy_and_Action_Plan_2016-2019_per_publikim_1202.pdf*.

171 European Commission Staff (2018). Kosovo* 2018 Report, p.29.

172 Kosovo* (2015). *National Cyber Security Strategy and Action Plan*, p.2.

173 RB32 interviewed between 25 and 30 June 2018 in Pristina

174 RB32 interviewed between 25 and 30 June 2018 in Pristina

175 RB34 interviewed between 25 and 30 June 2018 in Pristina

176 RB32 interviewed between 25 and 30 June 2018 in Pristina

177 RB32 interviewed between 25 and 30 June 2018 in Pristina

178 RB32 interviewed between 25 and 30 June 2018 in Pristina

179 European Commission Staff (2018). Kosovo* 2018 Report, p.12.

180 RB32 interviewed between 25 and 30 June 2018 in Pristina

181 RB32 interviewed between 25 and 30 June 2018 in Pristina

182 RB33 interviewed between 25 and 30 June 2018 in Pristina

183 RB33 interviewed between 25 and 30 June 2018 in Pristina

184 RB32 interviewed between 25 and 30 June 2018 in Pristina

185 RB32 interviewed between 25 and 30 June 2018 in Pristina

186 RB35 interviewed between 25 and 30 June 2018 in Pristina

187 RB35 interviewed between 25 and 30 June 2018 in Pristina

188 RB33 interviewed between 25 and 30 June 2018 in Pristina

by donors, to meet the commercial cyber security sector's needs. This appears to be a success, given the high percentage of employment after the programme. STIKK is also currently working with the government to establish a tech park, which would bring government stakeholders, experts, and businesses under one roof. This process has been developed strategically to ensure it meets current and future needs, with room for expansion and growth.[189] Nonetheless, there needs to be more cooperation between the public and private sectors, as well as input from academia, civil society, and the media. Unfortunately, there is not a large number of CSOs working in this space, which also needs to be addressed.

4.3.5 Assessment

As mentioned above, Kosovo's* laws and policies in this area are very good, but this progress is less evident in operational terms.[190] However, the government is aware of this and acknowledge in the National Cyber Security Strategy that challenges remain. They note one area in which this is very apparent, and this relates to technical aspect of cyber security or the lack thereof in many cases.[191] The Strategy further acknowledges that the police's cybercrime unit needs to be strengthened in the areas of resourcing, training, and international cooperation.[192] Other challenges also exist for the police, which include accessing trained personnel. Frequently new members to the unit have limited experience and have to be trained to an appropriate level before they can even start being productive. Furthermore, access to the necessary hardware and software is based on available resources, and these are often limited.[193] This lack of resourcing was also evident in other sectors of government,[194] where cyber security solutions are often available, but cost too much given their positioning in the private sector.

The provision of training for prosecutors and judges is improving. However, it was noted that this has not evolved at the necessary pace and therefore another review of the training module is needed.[195] It was further acknowledged that some judges and prosecutors are not sufficiently computer literate, so training and awareness raising needs to be much more basic for these.

4.4 Montenegro

As of December 2017, Montenegro had an internet user penetration level of 70%.[196] This has grown from 18.4% in 2000.[197] Speed and standards are in line with those experienced elsewhere in Europe.

4.4.1 Cyber Security Strategy

Montenegro's Law on Information Security was adopted in 2010 to act as umbrella legislation in the area of cyber security. This was reinforced by the development of a dedicated National Cyber Security Strategy for Montenegro 2013-2017. The accompanying action plan set out the establishment of the National Council for Cyber Security/Information Security, which was established in 2012.[198] In 2017, the government conducted an assessment of the old strategy and in December 2017, the Cyber Security Strategy of Montenegro 2018-2021 was published.[199] The government also adopted a multiannual strategy, based on the Digital Agenda for Europe and the EU's Digital Single Market strategy. This addresses, in addition to cyber security, issues such as accessibility of broadband services, digital business, e-health, and e-education.

The Montenegrin government ratified the Budapest Convention in March 2010 and appointed a 24/7 contact point. While this contact point has been recognised as useful, it is not being used as effectively as it might, given that formal cooperation processes have to be entered into if the cooperation goes beyond the exchange of advice and insight.[200] International cooperation in certain areas was deemed to be very good even at the government level. In certain highly skilled areas, international cooperation was considered to be priceless, given that economies often lack the necessary expertise internally.[201] Examples of good practice in the area of joint exercises were identified, such as participation together with CIRT/CSIRTs from across Europe in ITUs cyber drill activities in September 2015 and November 2017, which were supported and co-organised by the RCC. The iProceeds programme was also highlighted as beneficial in respect to both prosecutors and police.[202]

4.4.2 Government Agencies

Montenegro's first national cyber security strategy provided for the establishment of a national CIRT. This was originally located within the Ministry of Information Society and Telecommunications to act as a central body to coordinate and exchange information on and defend against cyber attacks. It was also responsible for raising awareness and for promoting a culture of cyber safety. However, after a change of government and consequent restructuring, it was moved to the Ministry of Public Administration.[203] Since taking over the area, the Ministry of Public Administration is trying to raise awareness amongst the public through campaigns, especially in the area of online child protection. The second national cyber security strategy was somewhat critical of the CIRT, acknowledging that it was the recognised focal point for responding to incidents, but noting that it lacked the specialised personnel required to successfully respond.[204] The first strategy also provided for the establishment of sector specific CIRTs. Many of these were not established during its lifetime, so this is a key activity within the new strategy.

In 2017, the government formed the Information Security Council.[205] The Council's tasks include:

To inform the Government of Montenegro on all important issues related to cyber security; monitor the implementation of the Cyber Security Strategy for Montenegro and the action plans for its implementation; monitor and coordinate activities in the field of cyber security; propose measures for harmonisation of the legislative and administrative frameworks in order to improve the cyber security of Montenegro; work to improve cooperation between state authorities and administrative bodies in the field of cyber security and coordinate their activities; work to improve cooperation with the private sector in the field of cyber security; submit its performance report to the Government of Montenegro at least once a year.[206]

A dedicated unit for High Tech Crime is responsible for investigating crimes that entail any element of cyber. This unit is based in the Ministry of Interior.[207] It most commonly investigates online child sex abuse and fraud related crimes, but also has responsibility for investigating cyber attacks, such as DoS, DDoS, and phishing incidents, amongst others.[208]

4.4.3 Incidents

Unlike in other economies in the region, some statistics are available in respect to cyber attacks in Montenegro. They are presented in Table 7. Nevertheless, many cyber attacks, as well as other cybercrimes, still go unreported and very few cases of cybercrime progress through to prosecution and the courts. Those that do are largely in relation to credit card fraud.[209] Few cases of online child sexual abuse and very few cases of cyber attacks on critical infrastructure go before the courts, our interviewees said.[210] This was reiterated in the EU's 2018 assessment, which stated that investigations into cybercrime, including online child sexual abuse, remain very rare.[211]

189 RB33 interviewed between 25 and 30 June 2018 in Pristina

190 RB36 interviewed between 25 and 30 June 2018 in Pristina

191 European Commission Staff (2018). Kosovo* 2018 Report, p.12.

192 European Commission Staff (2018). Kosovo* 2018 Report, p.12.

193 RB32 interviewed between 25 and 30 June 2018 in Pristina

194 RB32 interviewed between 25 and 30 June 2018 in Pristina

195 RB34 interviewed between 25 and 30 June 2018 in Pristina

196 Internet World Stats (2018). 'Europe'.

197 Internet Live Stats (2016). 'Montenegro Internet Users': *http://www.internetlivestats.com/internet-users/montenegro/*.

198 Per Montenegro's CIRT's official website: *http://www.cirt.me/O_Nama*.

199 Government of Montenegro (2017). *Cybersecurity Strategy of Montenegro*.

200 RB23 interviewed between 17 and 19 June 2018 in Podgorica

201 RB27 interviewed between 17 and 19 June 2018 in Podgorica

202 RB23 interviewed between 17 and 19 June 2018 in Podgorica

203 RB23 interviewed between 17 and 19 June 2018 in Podgorica

204 Government of Montenegro (2018). *Cybersecurity Strategy of Montenegro*, p.17.

205 Government of Montenegro (2018). *Cybersecurity Strategy of Montenegro*, p.14.

206 Government of Montenegro (2017). *Cybersecurity Strategy of Montenegro*, p.20.

207 RB23 interviewed between 17 and 19 June 2018 in Podgorica

208 RB23 interviewed between 17 and 19 June 2018 in Podgorica

209 RB31 interviewed between 17 and 19 June 2018 in Podgorica

210 RB31 interviewed between 17 and 19 June 2018 in Podgorica

211 RB23 interviewed between 17 and 19 June 2018 in Podgorica

YEAR	ATTACKS ON WEBSITES and IS	ONLINE FRAUD	ABUSE OF SOCIAL PROFILES	INAPPROPIRATE CONTENT ONLINE	MALWARE	OTHER
2013	5	3	10	-	1	3
2014	5	6	20	5	-	6
2015	6	17	37	19	17	36
2016	18	20	36	14	50	25
2017 (until Sept 1)	90	13	25	4	245	8
Total	124	59	128	42	313	78

Table 7 Statistics by year and type of attack in Montenegro.

Source: Government of Montenegro (2018). *Cybersecurity Strategy of Montenegro*, p.20.

4.4.4 Relationships between Public and Private Sector

The importance of PPPs was recognised as a priority in Montenegro's second cyber security strategy.[212] The strategy noted one example of where this cooperative approach has resulted in success, which related to the organisation of joint promotional campaigns on the protection of children in cyberspace and the safe use of the Internet.[213] Furthermore, given the CIRTs acknowledgement that malware was one of the biggest threats in Montenegro, a pilot project was launched that saw the cooperation of the Agency for Electronic Communications and Postal Services (EKIP) and Montenegrin internet providers. The project aimed to identify infected computers, and to take necessary action in response. Good cooperation was also reported between the police and the private sector, such as fraud departments in banks, ISPs, etc.[214] However, it was acknowledged that more needs to be done to progress this cooperation as many of these relationships are not at a sufficiently high level.[215]

It is acknowledged that the private sector in Montenegro is very progressive in the cyber security field, with some IT service providers pioneering in this area for at least 15 years.[216] Nonetheless, it is acknowledged that it is small, working largely on a project basis. A number of factors can make this market difficult for companies. Firstly, the lack of clear standards, meaning that competition is strong, largely driven by price not quality. Secondly, the private sector can be broken down into two areas, implementers – basically cyber security service providers – and users, such as banks, telecommunication companies, etc. Both need assistance. Service provision needs to be of a high quality and driven by security needs rather than price, whilst users need to better understand what services they require and why they need to invest. Both groups would benefit from governmental support, such as improved cyber security policy, practices, and standards.[217]

The field of cyber security is recognised as an important academic field in Montenegro.[218] However, only one dedicated programme is offered. This masters-level programme on cyber security policy has been developed by Donja Gorica University in Podgorica. This combines a mix of technical and policy-based knowledge on a variety of cyber security issues, with a view to providing a multi-disciplinary programme that attracts key stakeholders from both the public and private sectors.[219] An interesting aspect of this course is that it was designed to complement the level of capacity within the governmental institutions at the time, with the purpose of evolving as they do.[220] For example, it now includes important tuition on developing a strategic approach to cyber security, supported by the necessary policies, practices, and procedures. If this area progresses adequately, the course is designed to be flexible to change to a more technical programme.

212 RB23 interviewed between 17 and 19 June 2018 in Podgorica

213 RB30 interviewed between 17 and 19 June 2018 in Podgorica

214 RB23 interviewed between 17 and 19 June 2018 in Podgorica

215 RB27 interviewed between 17 and 19 June 2018 in Podgorica

216 RB24 interviewed between 17 and 19 June 2018 in Podgorica

217 *Ibid*.

218 RB28 interviewed between 17 and 19 June 2018 in Podgorica

219 *Ibid*.

220 *Ibid*.

Despite the above, many argue that the government is still not displaying the necessary levels of commitment to cyber security. For one, there is a lack of discussion around human rights and cyber security. This is perpetuated by a tradition of secrecy around security in Montenegro and in the region.[221] Government need to be held to account in the practices and policies they implement. The limited involvement of civil society in this area may exacerbate this, not holding the government to account. A number of factors influence this. For one, there is not the same tradition of CSOs in Montenegro as elsewhere within the region. Furthermore, public perceptions of some CSOs have been tainted due to their misuse of funds, use of CSOs by opposition parties, and other practices that make people question their commitment to the public good. Additionally, as elsewhere in the region, there is not much donor money in the cyber security realm hence not much activity, as the majority of CSOs are donor dependent.[222]

4.4.5 Assessment

Montenegro is progressing quickly in the area of cyber security from a legislative and policy perspective. In relation to chapter 24 of the *acquis*, the EU assessed that Montenegro is moderately prepared to implement the *acquis* in this area. They noted that the legal and strategic frameworks are now largely in place, but did not elaborate in the area of cyber security specifically.[223] In relation to chapter 10 of the *acquis*, the EU assessed that there is good functioning of the internal market for electronic communications and electronic commerce and audio-visual services. Overall it assessed that Montenegro continues to be moderately prepared in the area of information society. The same rate of progress was not evident at the operational level, but this is changing. [224] In theory, many report that things are good, but at the practical level things are less effective.[225] For example many sectors lack the necessary policies, standards, procedures, and practices. However, where they are present, they have been shown to work, such as in the finance sector, where cyber security practices have become an integral part of risk management and assessment processes.[226]

The lack of operational capacity is also evident when one looks at the police. For example, despite the presence of a dedicated unit to investigate cybercrimes and attacks, it is not resourced in the manner necessary for it to conduct its activities as designed. Such limitations are evident in the unit's manpower, access to qualified staff, and in respect to hardware and software infrastructure,[227] which together have translated into unfavourable conditions within the unit at present. This is also an issue in the private sector, despite attending university, graduates often require at least a year of practical training once employed to bring them to a reasonable standard.[228] Respondents also noted that it can be difficult to recruit experts to the public sector, given the wages, opportunities in the private sector, and recruitment criteria.[229] Challenges also exist from the perspective of prosecutors and judges. Whilst they are receiving training in this area and in other complimentary areas, such as digital evidence, the training has not always kept pace with their needs.[230] It was also noted that it can be difficult to put the learning into action given the small number of cases going through the system, which can be frustrating. [231] Criticism was also levelled at the administrative positioning of CSIRT, arguing that the Ministry for Public Administration is not the appropriate location,[232] with the previous system deemed better for citizens. In fact, it was noted that citizens do not know where to report incidents anymore. [233]

4.5 Serbia

As of December 2017, Serbia had an internet user penetration level of 72%.[234] This has grown from 12.3% in 2000.[235] Speed and standards are in line with those experienced elsewhere in Europe. However, despite this access, many Serbians still prefer to engage with the government via traditional means, despite a good level of e-government services, as

221 *Ibid*.

222 RB30 interviewed between 17 and 19 June 2018 in Podgorica

223 European Commission Staff (2018). *Montenegro 2018 Report*, p.29.

224 RB23 interviewed between 17 and 19 June 2018 in Podgorica

225 RB30 interviewed between 17 and 19 June 2018 in Podgorica

226 RB27 interviewed between 17 and 19 June 2018 in Podgorica

227 RB23 interviewed between 17 and 19 June 2018 in Podgorica

228 RB24 interviewed between 17 and 19 June 2018 in Podgorica

229 Rb27 interviewed between 17 and 19 June 2018 in Podgorica

230 RB30 interviewed between 17 and 19 June 2018 in Podgorica

231 RB31 interviewed between 17 and 19 June 2018 in Podgorica

232 RB23 and RB28 interviewed between 17 and 19 June 2018 in Podgorica

233 RB28 interviewed between 17 and 19 June 2018 in Podgorica

234 Internet World Stats (2018). 'Europe'.

235 Internet Live Stats (2016). 'Serbia Internet Users': *http://www.internetlivestats.com/internet-users/serbia/*.

acknowledged by the EU.[236] This lack of uptake is largely due to traditional culture, but could be improved by increased public awareness of the benefits of using online systems. It was also noted that there is a lack of trust in government institutions, which may have negative repercussions on e-government. Many citizens are detached from politics, the highest rates of which are amongst younger generations.[237] The government may benefit from working to restore trust and respect before they roll out additional online services, because they need to ensure accountability if people's information is leaked or trust may be further eroded. This is also likely to require additional awareness raising as many citizens are still largely unaware of the threats and risks associated with cyber activities, or at least do not see them as a priority.[238]

4.5.1 Cyber Security Strategy

Serbia adopted a Law on Information Security in January 2016. This law is the first overarching law regulating protective measures against security risks in information and communication systems, the liability of legal entities in the management and use of information and communication systems, and defining competent authorities for implementation of protective measures. The law also provided for the establishment of the National Centre for Prevention of Security Risks (CSIRT). However, in 2018, the EU assessment report noted that full harmonisation of the Law on Information Security with the NIS Directive is still pending. Under Chapter 24 of the *acquis*, and on a positive note, it was reported that the operational capacity in the Prosecutor's Office for Cybercrime had improved. Additionally, under Chapter 10 of the *acquis*, the report noted that Serbia is moderately prepared in the field of information society. Serbia also has a dedicated Cyber Security Strategy, which was adopted in 2017, but it lacks an associated action plan at present. However, great action in this area is most likely, given that as cyber security is one of six priority areas in the Strategy for the Development of Information Society in Serbia 2020.

The Government of Serbia ratified the Budapest Convention in April 2009. The 24/7 point of contact (PoC) was established in the Department for the Fight against High Tech Crime in the Ministry of Interior and Special Prosecutor for High Tech Crime. Cooperation at this level was considered to be good, but it was acknowledged that where mutual legal assistance was needed in regard to criminal matters, the competent authorities were the national courts and the public prosecutor's office, not the 24-hour PoC. International cooperation with regard to training and through the provision of experts was highly valued. One good practice identified in respect to this was joint table top exercises. Many considered these to provide valuable learning opportunities through both the exercises and through the exchange of learning and experience between participants. The UK, the Netherlands, and the EU were recognised for their input, as were other countries that have bilateral agreements with Serbia.[239]

4.5.2 Government Agencies

The national CSIRT is located in the Republic Agency for Electronic Communications and Postal Services (RATEL). Its key task is to coordinate prevention and protection from security risks in ICT systems in Serbia, on the national level.[240] It also has responsibility to coordinate responses to incidents and to raise awareness in this area, but it does not have competency to investigate incidents.[241] A number of other CSIRTs are also present in Serbia. These include AMRES-CSIRT (in the Academic Network of Serbia, for scientific and educational institutions), CSIRT MUP (in the Ministry of Internal Affairs) and SHARE CSIRT (in the non-profit foundation *SHARE*). In respect to policing, the Ministry of Internal Affairs established a dedicated police cybercrime unit within the Department for Fight against High Tech Crime. This unit investigates cyber attacks on government, private bodies, and on citizens. [242] A Special Prosecution Office for the fight against cybercrime was also established in 2005 and given greater responsibility in 2010.

4.5.3 Incidents

Like in other economies, it is difficult to provide statistics on cyber attacks in Serbia. The most well-known attack occurred in November 2014, when 19 files of more than 19 GBs were released and went viral via social networks. These documents contained more than 4,000 financial documents and endless lists of individuals' personal data. After investigation, it was determined that the document had been publically available for nearly ten months.[243] Smaller or lesser known attacks often go unnoticed, unreported, or are not investigated due to lack of technical capacity, resources, or a perception that such incidents will not result in prosecution. Those cyber attacks that have been detected have largely taken the form of DoS attacks and malware, many originating outside Serbia.[244]

4.5.4 Relationships between Public and Private Sector

Good cooperation exists between the private sector and government, for the most part, and it is improving, with an acknowledgement by many that formal PPPs are needed to ensure a more multi-disciplinary approach is achieved.[245] However, more needs to be done to build trust and cooperation between both sectors. This lack of trust can be seen in how, similar to other economies, many private sector organisations do not report cyber incidents when they occur. The lack of coordination and cooperation was attributed to a lack of awareness of what an effective national reporting system should look like. However, the banking sector was highlighted as an example of good practice, given the high level of cyber security embedded in its culture and good cooperation with government.[246]

A lack of strategic thinking on behalf of the government is also evident in the education sector. The available educational programmes are not commensurate with the needs of the market nor those of the government.[247] Explicitly, the education sector still lacks a multi-disciplinary approach to IT education, one which includes IT but also topics such as law, regulation, policy development, etc.[248] This gap results in a lack of experts who can translate technical knowledge into policy and practice.[249] This may be one of the reasons why there has yet to be a real strategic approach to cyber security in Serbia. It is also noted that more needs to be done at the national and secondary school levels.[250] Children need to be educated to be aware of the threats and risks posed in cyberspace, given they are active users of such technologies. That said, the Ministry of Trade, Tourism and Telecommunications does run a 'Smart and Safe' campaign to raise awareness of online safety for children, which is a start.

Progress has been achieved in relation to cyber security by CSOs, with a number working in the field of cyber security, unlike many other economies in the region[251] However, a lack of competent CSOs limits the oversight of government policies and practices, so this needs to be improved. One reason for the lack of activity in this area results from the fact that it is difficult to attract resources to this field.[252] Many CSOs are dependent on donor funds and if not available, such activities are often avoided, despite their merits. Discussions about the conjunction of cyber security and human rights are particularly limited.[253] Furthermore, it is acknowledged that advocacy, in this area, like others, is difficult, and can be slow.[254] On a positive note, efforts were made to establish a Civil Society CSIRT to help respond to attacks on CSOs and the media. While this has yet to be established, it could prove useful as a number of organisations reported that they have been the victims of cyber attacks.

4.5.5 Assessment

The area of information security is seen as a relatively new field of awareness for the Serbian government, but one that is becoming more mainstreamed.[255] It was acknowledged that legislation has improved and the government is aware that there is a need to build a better cyber security culture.[256] However, they have yet to adopt a strategic approach to cyber security or show a clear recognition of the threats and risks associated with cyber security to Serbia if left unaddressed.[257] This is exacerbated by limited operational capacity of government organisations in this area.[258] For example, it was claimed that the national CSIRT while formally established, lacks substance, despite eager and professional staff.[259] Secondly, it was acknowledged that the operational capacity of the Cybercrime Department of the Ministry of Interior is not as effective as it could be. It was noted that while the police are good, if not very good, with many head hunted by the private sector for their expertise, current resourcing does not allow

236 European Commission Staff (2018). *Serbia 2018 Report*, p.12.

237 RB21 interviewed between 13 and 16 June 2018 in Belgrade

238 RB18 interviewed between 13 and 16 June 2018 in Belgrade

239 RB18 interviewed between 13 and 16 June 2018 in Belgrade

240 See *https://www.cert.rs/en/stranica/57-O+Nacionalnom+CERT-u.html*

241 RB18 interviewed between 13 and 16 June 2018 in Belgrade

242 RB18 RB27 interviewed between 13 and 16 June 2018 in Belgrade

243 Rizmal, I., Radunović, V., and Krivokapić, D. (n.d.). *Guide Through Information Security in the Republic of Serbia*, Centre for Euro-Atlantic Studies (CEAS) and OSCE Mission to Serbia: https://www.osce.org/serbia/272171?download=true.

244 RB18 interviewed between 13 and June 2018 in Belgrade

245 RB18 interviewed between 13 and June 2018 in Belgrade

246 RB19 interviewed between 13 and 16 June 2018 in Belgrade

247 RB18 interviewed between 13 and 16 June 2018 in Belgrade

248 RB19 interviewed between 13 and 16 June 2018 in Belgrade

249 *Ibid*.

250 RB18 interviewed between 13 and 16 June 2018 in Belgrade

251 *Ibid*.

252 RB21 interviewed between 13 and 16 June 2018 in Belgrade

253 RB20 interviewed between 13 and 16 June 2018 in Belgrade

254 *Ibid*.

255 RB18 and RB20 interviewed between 13 and 16 June 2018 in Belgrade

256 RB19 interviewed between 13 and 16 June 2018 in Belgrade

257 *Ibid*.

258 RB26 interviewed between 13 and 16 June 2018 in Belgrade

259 RB18 interviewed between 13 and 16 June 2018 in Belgrade

for them to work at the necessary level.[260] It was suggested that this could be partially remedied by the establishment of special investigative units on credit card fraud, e-commerce and e-banking, and on combatting illicit and harmful internet content.

Progress has been made through increased operational capacity in both the Prosecutor's Office for Organised Crime and the Prosecutor's Office for Cybercrime. Both have received training, alongside judges, in this area.[261] However, it is acknowledged that it can be difficult to stay on top of emerging threats, especially given that it is hard to get experience of cases with a significant cyber component given the low numbers of cases reported.[262] As a result, there is still a capacity gap between current skill sets and where they need to be.[263] It was also noted that it can be difficult to recruit suitable staff within the government. Recruitment can be slow, bureaucratic, and the low salaries in comparison with the private sector make such jobs less attractive to many IT professionals. This results in a lack of access to suitable staff with the appropriate qualifications and experience.[264] Accepted too is that there needs to be greater synergy between a range of stakeholders, such as government, private sector, civil society, education, etc.[265] No significant progress can be achieved without it nor can it be achieved on enthusiasm alone, but this will require a shift in mind set to include a public-private partnership approach in this sector.[266]

4.6 The Former Yugoslav Republic of Macedonia

As of December 2017, the internet penetration level in The Former Yugoslav Republic of Macedonia was 76%;[267] an increase from 2.5% in 2000.[268] The Former Yugoslav Republic of Macedonia has undergone a rapid development of telecommunications and information society.[269] The fixed broadband penetration is comparatively low and not improving, impacting negatively on business competitiveness.[270] However, the EU in its 2018 assessment noted that the digitalisation of the economy is progressing fast. This development has allowed the government to pursue e-government services since 2009. This process was developed by the Ministry of Information Society and Administration, prioritising areas such as e-education, e-citizens, e-business, e-infrastructure, and information security. However, citizens often do not trust online systems, preferring to do things manually, especially when it comes to exchanging money or official information.[271] It was also highlighted that more needs to be done to educate citizens in this area, given a perceived lack of awareness and know-how.[272] Furthermore, it was claimed that the majority of citizens – and businesses too, for that matter – are very badly protected in the area of cyber security.[273]

4.6.1 Cyber Security Strategy

The Former Yugoslav Republic of Macedonia does not have an overarching law on cyber security. Nonetheless, it adopted its cyber security strategy in July 2018. In 2018, the EU in its assessment of The Former Yugoslav Republic of Macedonia noted that the criminal code is broadly in line with European standards, specifically noting that it criminalises online child sexual abuse and computer crime, amongst other crimes. It also recommends they prepare a long-term Information Communication Technology (ICT) Strategy. The assessment notes that The Former Yugoslav Republic of Macedonia is moderately prepared to implement the *acquis* under Chapter 24 of the *acquis*, but does not specifically mention cybercrime.

The Government of The Former Yugoslav Republic of Macedonia ratified the Budapest Convention in 2004. Complying with Article 35 of the Convention, the government appointed a 24/7 contact point, within the Office of the Public Prosecutor Department to combat against crime and corruption. This is supported by mutual legal assistance programmes. The Ministry of Justice is the designated central authority for this, at least with regard to criminal matters. The OSCE was identified as providing a lot of support to The Former Yugoslav Republic of Macedonia's CIRT, including running a national table top exercise in the area of cyber security. A wide range of organisations participated in the exercises, representing both public and private sectors.[274] These exercises were highly appreciated and deemed invaluable.[275] This was reiterated in respect to similar exercises run by ENISA and NATO. Respondents said The Former Yugoslav Republic of Macedonia would benefit from being a part of these exercises, which is not always possible given lack of membership.[276] Past support was also appreciated, such as the technical support of the ITU in relation to the establishment of the CIRT and participation in workshops and training programmes funded by the EU and NATO, such as the EU project CyberCrime@IPA and NATO Science for Peace and Security (SPS) advanced research workshops.[277]

4.6.2 Government Agencies

The Former Yugoslav Republic of Macedonia established its national CSIRT in 2016, which is situated within the Agency for Electronic Communications. The CSIRT represents the official national point of contact and coordination in dealing with network security incidents and risks, both nationally and internationally.[278] It has taken The Former Yugoslav Republic of Macedonia's CSIRT about 18 months to get up and running, but it is now actively building capacity. That said, it still faces a number of challenges, one of which relates to staffing. The unit is resourced for a workforce of five, but currently is at three, which means it is restricted in its ability to deliver all activities as set out in the work plan.[279] In the future, it is hoped that the CSIRT will be enhanced further to allow it to use advanced technologies that would enable, for example, malware analysis, which is limited at present.[280] Access to a dedicated lab would also enhance capacity and capabilities.[281] The work of the CSIRT is supported by the Cybercrime and Digital Forensic Department of the Ministry of Interior. If an incident is shown to be of a criminal nature, this unit investigates with the support of the CSIRT.[282] This unit resulted from a merging of the cybercrime unit within the Department for Suppression of Organised and Serious Crime with the Forensic Department of the Ministry of Interior, with the aim of improving efficiency and effectiveness.

4.6.3 Incidents

It is very difficult to get formal statistics in respect of cyber attacks and incidents in The Former Yugoslav Republic of Macedonia. Incidents are nevertheless occurring, with reports of several cases of defacement of institutional websites.[283] The lack of reports has a negative impact on the government's response, given that the risk is not felt and therefore cyber security is not high on the agenda. However, the response to cybercrime is different. It is on the rise and therefore has received more attention. A number of organisations interviewed reported direct experience of cyber attack. However, they noted that they did not report the incidents, based on a lack of confidence that they would be investigated and prosecuted. The majority of attacks were of DoS and phishing types, but malware distribution is increasing albeit there is a lack of awareness by many users of this threat.[284]

4.6.4 Relationships between Public and Private Sector

Cyber security is an area of priority for IT companies, but is less so for other sectors.[285] This has impacted the development of relationships between the public and private sectors in The Former Yugoslav Republic of Macedonia. However, some organisations would like to see better relationships and would support activities in this area, if the government were to request it.[286] Businesses are not afraid nor do they shy away from implementing policy where they see the benefits. This is evident with GDPR, whereby many companies from The Former Yugoslav Republic of Macedonia proactively sought to comply with this legislation to ensure they could continue trading with the EU.[287]

In respect to education in the cyber security sector, universities are turning out IT graduates, but the number is considerably lower than what is needed. Furthermore, some programmes are not producing graduates that meet the needs of the market when they enter the workforce.[288] This creates a significant gap between what is needed and what is available. This is further exacerbated by the amount of people migrating from The Former Yugoslav Republic of Macedonia, both new gradu-

260 RB19 interviewed between 13 and 16 June 2018 in Belgrade

261 RB26 interviewed between 13 and 16 June 2018 in Belgrade

262 *Ibid*.

263 RB20 interviewed between 13 and 16 June 2018 in Belgrade

264 RB18 interviewed between 13 and 16 June 2018 in Belgrade

265 RB24 interviewed between 13 and 16 June 2018 in Belgrade

266 RB26 interviewed between 13 and 16 June 2018 in Belgrade

267 Internet World Stats (2018). 'Europe'.

268 Internet Live Stats (2016). 'Republic of Macedonia Internet Users': *http://www.internetlivestats.com/internet-users/macedonia/*

269 Tasevski, P. (2015). 'Macedonian Path Towards Cyber Security', Information & Security: An International Journal, 32(5).

270 European Commission Staff (2018). *The Former Yugoslav Republic of Macedonia 2018 Report*, p.50.

271 RB39 interviewed between 27 and 30 June 2018 in Skopje

272 RB42 interviewed between 27 and 30 June 2018 in Skopje

273 *Ibid*.

274 RB41 interviewed between 27 and 30 June 2018 in Skopje

275 RB38 interviewed between 27 and 30 June 2018 in Skopje

276 *Ibid*.

277 *Ibid*.

278 Per the official website of The Former Yugoslav Republic of Macedonia's CIRT: *https://mkd-cirt.mk/?lang=en*.

279 RB38 interviewed between 27 and 30 June 2018 in Skopje, The Former Yugoslav Republic of Macedonia.

280 *Ibid*.

281 *Ibid*.

282 *Ibid*.

283 Stojkovski, F. (2016). 'Macedonia Must Develop a Cyber Security Strategy', *Analytica*, Vol. 5: *https://www.analyticamk.org/images/Files/Commentary/2016/comment_extra5_en_85e95.pdf*.

284 RB38 interviewed between 27 and 30 June 2018 in Skopje

285 RB40 interviewed between 27 and 30 June 2018 in Skopje

286 RB42 interviewed between 27 and 30 June 2018 in Skopje

287 RB40 interviewed between 27 and 30 June 2018 in Skopje

288 RB42 interviewed between 27 and 30 June 2018 in Skopje

ates and experienced IT professionals. As a result, various associations are supporting processes that allow for re-qualification and re-training in the IT sector to help fill the vacuum.[289] This is indicative of the need to be flexible and creative in regards to mitigating brain drain from this economy.

Similar to other economies in the region, CSOs are limited in this area.

4.6.5 Assessment

It was asserted that The Former Yugoslav Republic of Macedonia's government is aware of the risks to which it is exposed from a cyber perspective, but does not have the capacity, in terms of technology, staffing, financial resources, etc. to address the risk effectively.[290] Others argued, on the other hand, that there is actually a significant lack of awareness within the government as regards the risks of cyber insecurity. This lack of awareness was also said to be present amongst citizens.[291] The EU noted in its 2018 assessment that relations between prosecutors, the police, and other relevant bodies and agencies need to be improved so that the prosecution service can fully play its lead role in investigations. For example, the Public Prosecutor's Office is not resourced at the level it should be. However, progress was also noted, with the EU reporting that "a package of amendments to several laws and a new law on an Operational Technical Centre, to reform the system for intercepting communications were adopted by the government in December 2017".[292] This will enable the establishment of a new independent agency, the Operational Technical Agency (OTA). The OTA will act as an:

"Intermediation body between the telecom operators and the authorities authorised to intercept communications for protection of the interest of security and the defence of the state and for the purpose of criminal investigations. Each authorised authority will intercept communications under its competences, following a court order".[293]

289 *Ibid*.

290 RB41 interviewed between 27 and 30 June 2018 in Skopje,

291 RB42 interviewed between 27 and 30 June 2018 in Skopje

292 European Commission Staff (2018). *The Former Yugoslav Republic of Macedonia 2018 Report*, p. 35.

293 *Ibid*.

5. FINDINGS AND RECOMMENDATIONS

While there has been significant progress in the WB6 with respect to harmonisation of legislation dealing with cyber security in line with, particularly, the EU framework, implementation is a different matter. Deficiencies in the area of funding, staffing, and technological advancement within government agencies tasked in this area, amongst other challenges identified above, contribute to this gap between what appears on paper and what is being done in practice. In terms of explanations for this gap, respondents felt strongly that there is a lack of awareness amongst political and other high-level decision makers of the magnitude of the risk and what needs to be done to mitigate it. Having said this, there is increasing awareness, including among mid-level decision makers in a diversity of sectors that cyber security needs to be moved up priority lists. This is coupled with a significant level of expertise and commitment within the WB6's public and private sectors that, if leveraged, could significantly improve implementation of cyber security measures. At the regional level, a more strategic approach to cooperation and the establishment of a cyber security centre of excellence are recommended. This will be discussed further below.

Recommendations aimed at resolving the above and a variety of other issues already raised in this report are provided in the below, which is divided into national- and regional-level sub-sections. These were derived from the findings of the research and through discussions with experts and stakeholders. Five recommendations aimed at WB6 governments are supplied. Three of these need to be addressed immediately; these are (i) the resourcing of agencies and units responsible for implementing economies' cyber security strategies and action plans so that they can be effectively executed; (ii) increased awareness-raising around cyber security issues (including cyber influence operations); (iii) leveraging of existing WB6-based cyber security expertise. Slightly longer term are the suggestions to (iv) not just talk about, but actually establish a range of PPPs and (v) engage in a wholesale review of cyber security education with a view to future-proofing it.

5.1 National-level recommendations

Despite progress in each of the WB6 with regard to cyber security, more needs to be done. The following recommendations should assist in achieving this.

5.1.1 Resource strategies and action plans

The main deficiencies identified in respect of cyber security strategies and action plans relate to the lack of investment to support the proper implementation and enforcement of the respective legislation and strategies. This needs to be addressed as a matter of priority to ensure progress maintains pace with advances in this sector, including significant and fast-paced advances by threat actors. The upshot of continued under-funding will not only be increased cybercrime, it will also negatively impact government policies such as information society, e-government, etc. The ability to develop and expand cyber security expertise is heavily impacted by available resources, without which little can be achieved.[294] A first step to concretely addressing this is to cost strategies and actions plans during the planning phase and then to reinforce such plans with dedicated funds. Solely relying on existing resources and/or donor funds will have significant negative impacts. Where funds are not available within economies, PPPs may provide a suitable alternative. Proper resourcing, through whatever means, will improve the immediate response capacities of police, CSIRTs, digital forensics units, etc., but will also enable activities such as prevention programmes, the conduct of regular threat assessments, and development of greater situational awareness, whilst also thinking more strategically long-term.

5.1.2 Create and/or improve reporting structures

The reporting rate of cyber security incidents needs to be improved. One method to do this is to make it easier for citizens and businesses to report such incidents. Many companies noted that they did not know how to report an incident, what information they would have to supply, and what and how much they could choose not to divulge. It is therefore recommended that CSIRTs reach out to such organisations and inform them about reporting processes and the nature and type of information that needs to be provided. This is already occurring in The Former Yugoslav Republic of Macedonia, where the CSIRT is trying to increase trust between them and the private sector to encourage reporting. In addition, Albanian police have established an online system for citizen reporting. When reports are made, of course, strict protections need to be in place to ensure sensitive information is not made public. However, this should not stop the public reporting of statistical data as such information is vital in understanding emerging patterns, trends, points of failure, and similar, which is integral to future planning. An added bonus may be that as individuals and companies become more aware of others reporting cyber security incidents, they too may be more willing to do so.

294 RB12 interviewed between 11 and 21 June 2018 in Sarajevo, BiH.

5.1.3 Raise awareness

All respondents noted the need for increased awareness on the part of citizens as regards their individual cyber security including, particularly, in respect to their right to privacy and related freedoms. In fact, there was little evidence that such debates are currently mainstream in the WB6, yet they need to be. This could be addressed through a number of different measures, including through formal education and professional training. However, CSOs, community groups, and private sector providers should also be supported to provide information and knowledge in this area, to ensure a multi-layered approach. In light of increased reference to surveillance, fake news, extremist content, cyber terrorism, etc., awareness raising campaigns and activities should also include critical thinking elements, so users develop the skills to look beyond the message *per se* and think about the sender, their interests, etc. in order to identify possible risks. More attention is given to these issues in Vol. 2 of this study.

Awareness-raising should also be conducted with donors, as they significantly influence the work of CSOs. Without the inclusion of CSOs, oversight is limited, which may have significant impact on human rights, if not properly monitored. On the other hand, awareness raising amongst political elites and policy makers is also desirable.

5.1.4 Leverage existing expertise

IT experts cannot be produced overnight, and while it is acknowledged that it can be difficult to access trained professionals, due to migration, lack of funds, competitive markets, etc., experts *are* available in the WB6 and things can be done to improve their situation. Creating networks of interested parties, such as the informal network initiated by OSCE and implemented by the Diplo Foundation and DCAF in Belgrade, or drawing on existing associations, such as those within the private sector, could be a very productive step. Furthermore, such networks of experts could assist in developing a more strategic approach to cyber security given their broad range of perspectives, experience, and vision. One specific example of where such expertise could be useful relates to GDPR. As mentioned above, many private sector businesses in the WB6 are GDRP compliant so they can continue to trade into the EU. Accession and harmonisation of legislation in this area, while not required by WB6 economies yet, will be necessary. The existing knowledge and experience within the private sector should be harnessed to ease the process at the economy level. This would also be beneficial to citizens as their protections as enshrined in GDPR, which if implemented may help instil greater trust, which may in turn lead to increased use of e-government and electronic services. Furthermore, being GDPR compliant as an economy is likely to be an attractive factor to investors.

5.1.5 Identify and develop PPPs and build synergies

Effective strategies in all policy realms are built on collaboration. Instead of just acknowledging the need for PPPs within cyber security (and CVE strategies; see Vol. 2), significant effort should be put into what such partnerships could look like and the areas that may most benefit from their establishment. Joint trainings are an obvious first step to building better relationships. For example, in cybercrime investigations, key evidence is often held by private industry; there are variety of avenues of legally obtaining this depending on the context. Representatives from law enforcement, companies, and others involved in these processes could usefully exchange information about their policies and procedures in this regard. The ultimate goal should be to maximise existing relationships and create synergies between stakeholders, which can oftentimes be achieved at low cost.[295] Worth noting here is that this will require commitment, support, and hand holding in the early days as trust and confidence take time to develop within such groups; this is a phase that is often overlooked, but that is critical to sustainability of such partnerships. The development of PPPs is therefore a longer term project, as is the development of more effective educational strategies.

5.1.6 Review educational approach to ICT and Cyber Security

The WB6 need to undertake a comprehensive review of its educational approach to ICT and cyber security. This should not only enquire into what courses are required and at what levels, but it needs to include a longer term assessment of future needs in this area, and courses developed and offered based on this. This should almost certainly include development of not just technology-based, but multi-disciplinary programmes to insure the competencies to support better strategic and operational implementation of cyber security strategy are available. Specific skill sets that might be looked at in the review include how to write, plan and cost strategy documents; how to conduct needs assessments of government departments and the private sector in respect to cyber, for now and into the future; and how to assess economic forecasts, development plans, etc. in respect to ICT development, just to highlight a few.

295 RB20 interviewed between 13 and 16 June 2018 in Belgrade, Serbia.

5.2 Regional-level recommendations

Many respondents agreed that progress in cyber security would benefit from a more joined-up and forward thinking regional approach, which would build on the work and structures of existing regional institutions, such as the RCC. This regional approach would be better use of scarce responses. Furthermore, it would illustrate a shared political will and proactivity in this area.

5.2.1 Develop more strategic approach to regional cooperation

It is recommended that developing a strategic approach to cyber security should be done within existing frameworks, such as that of the EU, rather than creating new ones. For example, develop a WB6 regional cyber strategy, which identifies and sets out regional critical infrastructure, common minimum standards, a CIWIN, etc. This will help mitigate risk and protect CII together. While this may appear to be replication of the work of the EU, accession will take time, driving this at the regional level can begin immediately and will only have a net benefit, if and when accession occurs. Advice and support should be garnered from ENISA and ITU to do this to ensure consistency and existing good practice are built upon. For example, greater sharing of existing expertise and good practice around developing workable cyber security policies and procedures, building on existing connections in areas such as electric power, and continue improving cooperation between law enforcement, prosecutors, and judges. ENISA, RCC, and NATO were all identified as potential facilitating partners in this increased cooperation. Economies such as Albania and Montenegro could pro-actively bring back learnings from NATO, where possible, to conduct regional exercises, which are much sought after. Such an approach would take considerable funding, economies will have to be willing to invest. Donor funding may be able to support this regional approach, but without willingness on behalf of all economies this is likely to fail or be limited in what it can achieve. The im-

petus for progress in this area needs to come from within, so it can be self-sustaining into the future. That said, donor support, in terms of finance, training, and knowledge sharing, especially from the EU and EU Member States, should be encouraged.

5.2.2 Realign support of the international community to the strategy of the region

The support of the international community is valued in this area, as in others, but does not come without criticisms, as was noted earlier. There is a need for greater discussion about what areas may benefit from such support, what support would have the greatest impact, and related issues. Having a regional strategy would help identify these areas and in so doing, identify where best to direct such support. This may help alleviate criticisms about duplication of resources and streamline programmes into priority areas for the region. This may also result in more meaningful impacts, instead of smaller projects being implemented at the economy level. An organisation, such as the RCC, could oversee this, ensuring the best use of funds within the region based on the needs and requirements within the strategy. Furthermore, things move quickly in this area, having a regional approach dictating where support should be provided may increase the timeliness of support, which would alleviate criticisms that some programmes are outdated by the time they are implemented.

5.2.3 Establish a regional centre of excellence

Many respondents noted that they were hindered by a lack of technical capacity to conduct their roles effectively. This was reported in CSIRTs, the police, digital forensics, etc. It was noted too that while twinning projects and the provision of training and mentoring are valuable, their true value cannot be garnered because of a lack of hardware, software, and other logistical necessities. As a result, some suggested a shared WB6 regional centre of excellence in cyber security would be of benefit. While this would not negate the need for basic, yet effective, minimum standards of equipment and technology at the economy level, more elaborate technology and equipment could be housed within a regional centre of excellence. This would reduce the cost on individual economies, yet provide them direct access to the technology, support, expertise, etc., as and when needed. One element could include acting as a linchpin for all national CSIRTs, by hosting a regional CSIRT within it. This would ensure sharing of information, expertise, and knowledge. Furthermore, positioning the centre with close alignment to a university could provide high end educational programmes, training, and research in this area. It could also house a regional institute or 'think tank', one looking at the future, but from a regional perspective, drawing on the work at the economy level, and influencing policy and long-term thinking. This would also position it well as a suitable body to identify opportunities for PPPs at the regional level.

It should be noted that many of the recommendations made above are consistent with those made by the Diplo Foundation in 2016. This in itself is indicative of a slow pace of change, but it also raises the question 'Are the WB6 really committed to cyber security?' The findings of this report suggest conflicting results. A lot of questions still remain unanswered or, at least from the outside looking in, appear to require clarification. These require an open discussion between politicians, bureaucrats, citizens, and the private, education, and civil society sectors to be answered, because they require real will, effort, and commitment to resolve. As these questions are answered, many more will surface. However, this process is necessary to ensure cyber security, in all its guises, risks, and challenges mainstreamed in areas such as democracy, governance, markets, and human rights. Such questions might include:

- Is cyber security a priority of WB6 economies, beyond EU accession and harmonisation of legislation, and what does this mean for WB6 economies?
- Is cyber security viewed as a formality or through the complex lens that it requires?
- If the latter, are WB6 economies willing to invest the necessary funds and resources in this area and how and where are they going to get such funds?
- Will cyber security be funded, at the economy level, regionally, or will it be dependent on donor funds? What are the likely impacts of such decisions?
- Are WB6 economies aware of the impact of each of these decisions and is there a willingness to live with the possible outcomes? What precautions need to be taken to minimise possible risks?
- Is the lack of PPPs, despite reference to them in many WB6 strategies, an indication of a lack of awareness of what multidisciplinary and multi-stakeholder approaches actually require?
- If the necessary response is not forthcoming from the public sector, is there a willingness and/or demand within other sectors to drive the necessary change?
- Are the WB6 ready to move beyond cyber security as a risk to discussions involving, impact on human rights, privacy rights, and freedoms?

Chapter 2

ONLINE RADICALIZATION IN THE WESTERN BALKANS

EXECUTIVE SUMMARY

This is the second volume of a two part study, which aims to provide a comprehensive overview and analysis of the situation as regards cyber security in Albania, Bosnia and Herzegovina, Kosovo*[1], Montenegro, Serbia and The Former Yugoslav Republic of Macedonia (hereafter WB6). Volume 1 addressed traditional cyber security concerns; this volume aims, ambitiously, to expand our understanding of cyber security beyond such traditional narrow perspectives to include information operations, with a focus in this report on online radicalisation.

In particular, this report conceives of online extremism and radicalisation as examples of information operations, which are treated as a cyber security issue. It also examines what needs to be done in order to mitigate existing and potential threats and risks associated with increased (malicious) users and targets from an information operations perspective.

In terms of approach, both desk based research and field consultations were conducted. A broad range of stakeholders were interviewed, from government, donor communities, the private sector, civil society and academia, to ensure differing perspectives were represented.

Similar to many EU countries, the WB6 conceive of cyber security narrowly and thus oftentimes responses to 'hard' attacks (i.e. cyber attacks, including cybercrime) are privileged over 'soft' (i.e. 'fake news', online radicalisation, etc.). When extremism and terrorism are taken into account, threats are often portrayed via worst case scenarios, from using cyber means to shut down the electric power grid to contaminating a major water supply. This approach has ignored what has thus far turned out to be the greater threat: everyday extremist and terrorist use of the internet to communicate, collaborate, and convince.

Emphasised in this report therefore is that attacks on cognitive infrastructure – on people, society and systems of information and belief – often referred to as information operations or information based attacks are coming more to the fore, as malicious actors use online systems to exploit heretofore largely ignored vulnerabilities in our information sphere.

1 *This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo declaration of independence.

Findings and Recommendations

Unlike with traditional cyber security concerns where the driving force behind WB6 activity is the European Union, by way of the Cyber Security Strategy of the European Union, NIS, and the Digital Agenda for Europe, amongst others, the driving force in relation to online radicalisation and extremism in the WB6 - similar to the EU and other regions globally - stems from the perceived risk posed by the emergence of the so-called 'Islamic State' (IS) and their online strategy. This resulted in all but two economies within the WB6, publishing national-level strategies for countering radicalisation and/or violent extremism. Only Bosnia and Herzegovina and Serbia have not yet published such strategies. That said, their counter terrorism strategies do reference use of the internet for terrorism or radicalisation purposes.

Nonetheless, the European Union does play a role in WB6 activity in this area, in terms of the influence of documents such as the European Union Counter-Terrorism Strategy, the EU Strategy for Combating Radicalisation and Recruitment to Terrorism, the EU Code of Conduct on Countering Illegal Hate Speech Online, the Joint Action Plan on Counter-Terrorism for the Western Balkans, the European Agenda on Security, the Council Conclusions on EU External Action on Counter-terrorism and the High-Level Commission Expert Group on Radicalisation (HLCEG-R). In respect to legislation, the EU Counter Terrorism Directive also has a role. It is also likely that the forthcoming EU rules on removal of online terrorist content will also be influential. EU bodies, such as the European Union Internet Forum, the EU Internet Referral Unit (EU IRU), and Radicalisation Awareness Network (RAN) were also found to have an impact in this area. Whilst a variety of documents and actors outside of the EU also play a role, including the OSCE, Council of Europe, the Global Internet Forum to Counter Terrorism, United Nations Security Council Counter-Terrorism Committee (UNCTC), and NATO.

Despite the presence of strategies and legislation addressing the intersections of extremism, terrorism, and the Internet in the WB6, there is a lack of progress in operationalising these. As a result, concern exists amongst policy makers, police, prosecutors, and others across the region regarding the role of the internet in radicalisation processes and potential threats posed. Unsurprisingly, the deficits associated with implementation and operationalisation of practical responses, are similar to those identified in Vol. 1 of the study regarding more traditional cyber security issues. The most significant of these include (i) limited resourcing of bodies, such as police and prosecutors, in respect of staffing, technology, and training, which is negatively impacting investigations; (ii) limited appropriate civil society participation; (iii) lack of significant public-private partnerships; (iv) lack of educational policies and programmes on identifying risky online content; and (v) the need for more careful media reporting.

Recommendations

Similar to Vol. 1, the following recommendations are provided to help address these challenges and to maximise progress in relation to the harmonisation of laws, strategies, and actions plans. Suffice to say that the recommendations in Vol. 1 are also applicable in this area.

National-level recommendations

Despite progress in each of the WB6 with regard to online radicalisation and extremism, more needs to be done. The following recommendations should assist in achieving this.

Review countering violent extremism strategies to ensure greater alignment with the EU Strategy for Combating Radicalisation and Recruitment to Terrorism

It is recommended that each of the four economies with countering violent extremism (CVE) strategies review them to ensure greater alignment with the EU strategy. It is also recommended that both Bosnia and Herzegovina and Serbia ensure alignment with this strategy when they finalise their CVE strategies.

Review counter terrorism and countering violent extremism strategies to ensure consistency and complementarity with cyber security strategies

It is recommended that each economy review their counter terrorism and countering violent extremism strategies to ensure their consistency with and complementarity to their cyber security strategies, as is the case with both EU strategies. This will also enable greater alignment at the operation level and better use of resources, if implemented properly. This may involve the need for awareness raising to illustrate the synergies between both areas.

Review strategies and legislation in the area of counter terrorism to ensure attacks on information systems are included

It is recommended that all economies' strategies and legislation in the area of counter terrorism include mention of attacks on information systems and that law enforcement and prosecutors have adequate response capabilities in this regard.

Review current relationships with Private Sector Companies, Civil Society Organisations, and the Media, and develop specific actions to improve the same

It is recommended that each economy conduct a scoping exercise to identify key organisations in the private sector, civil society, and the media and actively engage with them to develop better shared responses to online radicalisation and extremist content. Furthermore, it is recommended that these activities are included in their actions plans, which would go some way to ensuring that such objectives are achieved.

Introduce critical thinking into cyber security education

It is recommended that the WB6 introduce critical thinking components into the education curriculum. This will help create greater societal resilience to future information operations campaigns. Improved critical thinking skills are not just generally desirable, but should cause users to be more critical of extremist and terrorist content, which would be positive.

Regional-level recommendations

Ensure a consistent approach to extremism and extremist and terrorist online content

It is recommended that additional research is conducted that extends beyond jihadist online content, to include extreme right and nationalist content, whilst also being mindful of other emerging extremist content, so a more balanced picture is produced in this regard. This analysis might be best conducted at the regional level given that findings suggest the circulation of online content between economies. This may be best undertaken by the regional centre of excellence recommended in Vol. 1.

Take an intelligence and evidence-based approach

Wiping the Internet of all terrorist content is a seemingly impossible task. Nonetheless, making such content increasingly difficult and costly (i.e. in terms of time, know-how, etc.) to locate is a worthwhile pursuit that could be entered into by authorities in partnership with social media and other internet companies. A complementary approach is one driven by intelligence that is also evidence-based. This requires cooperation between law enforcement, tech companies, and ISPs to map networks, identify capabilities, and highlight potential content of interest, be it related to actors, targets, methods, etc. While such an approach may necessitate taking down content, it can be much more targeted to disrupt key relationships.

Develop better relationships with major tech companies

Contacts with major internet companies should be developed to understand how WB6 economies can better work together with them to monitor and respond to extremist content, before having to go down the road of legislative change. Furthermore, WB6 economies should look at building relationships and involvement with forums such as the EU Internet Forum and the Global Internet Forum to Counter Terrorism (GIFCT), with a view to creating a Western Balkans Internet Forum (EUIF) similar in structure and design to the EUIF, but focusing on content produced in Western Balkan languages.

Establish a Western Balkans Referral Unit

Similar to the EU IRU, a Western Balkans referral unit could have significant impact on online content produced in Western Balkan languages. Given that the EU IRU only has limited capacity in these languages, a WB6 version of the EU IRU would be complimentary to the EU IRU and as a result, the EU IRU may be willing to support the development of such a unit.

Develop and adopt a Western Balkans Agenda on Security

It is recommended that a Western Balkan Agenda on Security be developed and adopted at the regional level. Similar to the Digital Agenda for the Western Balkans, mentioned in Vol. 1, this approach could be used to support a regional approach to security, including online extremism and radicalisation. Having a detailed Agenda based on regional needs would be likely to ensure more structured direction of donor funds, reduce overlap and duplication, and enable the WB6 to maximise the benefits of shared resources.

Develop a Western Balkan version of the Radicalisation Awareness Network

The Radicalisation Awareness Network (RAN) is recognised within the WB6 as an excellent resource for information, expertise, and knowledge sharing at the EU level. Given the wealth of knowledge within the region, a similar network established in the region would be an excellent way to bring together experts, good practice, and advice on problem solving from a regional perspective. It is recommended that advice and support be garnered from the RAN to support this.

ORGANISATIONS INTERVIEWED

Interviews were conducted with representatives from the following organisations. Their time, insights and opinions are greatly appreciated.

- Academy of Justice, Kosovo*
- American Chambers of Commerce, The Former Yugoslav Republic of Macedonia
- Balkan Investigative Reporting Network (BIRN)
- Belgrade Centre for Security Policy (BCSP), Serbia
- Bit Alliance, Bosnia and Herzegovina
- Boga & Associates, Law Firm, Albania
- Center for Democracy and Human Rights (CEDEM), Montenegro
- Center for Free Elections and Democracy (CESID), Serbia
- Center for Investigative Journalism SCOOP, The Former Yugoslav Republic of Macedonia
- Central Bank, Montenegro
- Centre for Security Studies, Bosnia and Herzegovina
- Cyber Security Specialist, The Former Yugoslav Republic of Macedonia
- DCAF, Serbia
- Diplo Foundation, Serbia
- European Movement in Albania
- General Directorate of State Police, Department of Economic Crime, Albania
- Institute for Democracy and Mediation (IDM), Albania
- IT Specialist, Albania
- IT Specialist, Bosnia and Herzegovina
- IT Specialist, Kosovo*
- Kosovo* Centre for Security Studies
- Kosovo* Forensics Agency
- Chamber of Information and Communication Technologies (MASIT) - ICT Chamber of Commerce, The Former Yugoslav Republic of Macedonia
- Melita Partners, Kosovo*
- Ministry of Defence, Bosnia and Herzegovina
- Ministry of Energy and Infrastructure, Albania
- Ministry of Internal Affairs, Montenegro
- Ministry of Security, Bosnia and Herzegovina
- CIRT, National Authority for Electronic Certification and Cyber Security, Albania
- National Computer Incident Response Team (-CSIRT), The Former Yugoslav Republic of Macedonia
- NESECO, Bosnia and Herzegovina
- Organized Crime and Corruption Reporting Project (OCCRP)
- Organization for Security and Co-operation in Europe (OSCE) Albania
- OSCE, The Former Yugoslav Republic of Macedonia
- OSCE, Serbia
- Republic Agency for Electronic Communications and Postal Services, Serbia
- S&T, Montenegro
- Specialist on Radicalisation, The Former Yugoslav Republic of Macedonia
- State Prosecutors of Montenegro
- The Centre for Training in Judiciary and State Prosecution, Montenegro
- ICT Association, Kosovo*
- Tirana Prosecution Office, Albania
- Towersnet, Serbia
- University of Donja Gorica, Montenegro
- University of Pristina

LIST OF ABBREVIATIONS

AHT	Albania Hacker's Terrorist
ALCIRT	Albanian National Agency for Cyber Security
AKCESK	National Authority for Electronic Certification and Cyber Security
AKSHI	National Agency for Information Society
AMC	Albanian Muslim Community
AMRES	Academic Network of Serbia
BiH	Bosnia and Herzegovina
BSF	Belgrade Security Forum
CDCT	Committee on Counter Terrorism
CEAS	Centre for Euro-Atlantic Studies
CEF	Connecting Europe Facility
CII	Critical Information Infrastructure
CIP	Competitiveness and Innovation Programme
CIWIN	Critical Infrastructure Warning Information Network
CODEXTER	Committee of Experts on Terrorism
CSDP	Common Security and Defence Policy
CSIRT	Computer Emergency Response Team
CSO	Civil Society Organisation
CVE	Countering Violent Extremism
DAE	Digital Agenda for Europe
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DDoS	Distributed Denial-of-Service
DOS	Denial of Service
DSIs	Digital Service Infrastructures
EC	European Commission
ECI	European Critical Infrastructure
EC3	Europol's Cybercrime Centre
ECTC	Europol's European Counter Terrorism Centre
EKIP	Agency for Electronic Communications and Postal Services
ENISA	European Union Agency for Network and Information Security
ESI	European Structural and Investment
EU	European Union
EUIF	European Union Internet Forum
EUIRU	Europol's Internet Referral Unit
FP7	7th Framework Programme
GCA	Global Cybersecurity Agenda
GDPR	General Data Protection Regulation
GIFCT	Global Internet Forum to Counter Terrorism
HLCEG-R	High-Level Commission Expert Group on Radicalisation
H2020	Horizon 2020 Research and Innovation Framework Programme
IAP	International Association of Prosecutors
ICITAP	International Criminal Investigative Training Awareness Program
ICM	Islamic Community of Montenegro
ICT	Information and Communication Technology
IED	Improvised Explosive Devices
IISG	Integrative Internal Security Governance
IMPACT	International Multilateral Partnership against Cyber Threats
IOCTA	Internet Organised Crime Threat Assessment
IOM	International Organisation for Migration
IoT	Internet of Things
IP	Internet Protocols
IPA	Instrument for Pre-accession Assistance
IS	Islamic State
ISF	Internal Security Fund
ISP	Internet Service Providers
ITU	International Telecommunication Union
JHA	Justice Home Affairs
MAP REA	Multi-Annual Action Plan for a Regional Economic Area in the Western Balkans
MARnet	National Academic and Research Network
MIT	Massachusetts Institute of Technology
MOU	Memoranda of Understanding
NCCVECT	National Committee for Countering Violent Extremism and Countering Terrorism
NAEC	National Authority for Electronic Certification
NATO	North Atlantic Treaty Organization
NBS	National Bank of Serbia
NGO	Non-Governmental Organisations
NIS	Network and Information Security Directive
OTA	Operational Technical Agency
PCVE	Preventing and Countering Violent Extremism
POC	Point of Contact
PPP	Public-Private Partnership
RAN	Radicalisation Awareness Network
RATEL	Republic Agency for Electronic Communications and Postal Services
RCC	Regional Cooperation Council
R&D	Research and Development
RUSI	Royal United Service Institute
SIPA	State Investigation and Protection Agency
TDO	The Dark Lord
TSO	Transmission System Operators
UK	United Kingdom
UN	United Nations
UNCTC	United Nations Counter Terrorism Committee
UNCTED	United Nations Counterterrorism Executive Directorate
UNDP	United Nations Development Programme
UNODC	United Nations Office on Drugs and Crime
WBBSi	Western Balkan Border Security initiative
WBCSi	Western Balkan Counter Serious Crime initiative
WBCTi	Western Balkan Counter-Terrorism initiative.

1. INTRODUCTION

Information operations or information-based attacks focus on "cognitive infrastructure, on people themselves, on society, and on systems of information and belief".[2] The power of disinformation and misinformation to manipulate narratives is increasingly to the fore of late, especially in the context of so called 'fake news'. A wide variety of malicious actors, from states with traditional geopolitical interests to financially-motivated information entrepreneurs to extremists and terrorists, are today weaponising the Internet, particularly social media, to forward their goals.

Terrorism has always been about communication because, as Schmid and De Graaf (1982) stated over thirty five years ago now, "without communication there can be no terrorism".[3] In a similar vein, the late British Prime Minister Margaret Thatcher famously described publicity as the oxygen of terrorism. This pronouncement continues to resonate and while it is never their ultimate objective, publicity is what sustains effective terrorist campaigns. It follows from this that extremists and terrorists should take every opportunity to get their message out to as large an audience as possible by amplifying their violence via all available media channels. And, as Ranstorp put it just over a decade ago, "[t]he role of the media as the oxygen of publicity would take on a new added meaning, urgency and complexity with globalisation and the instruments of cyberspace".[4] Interestingly however, the intersections of 'cyber' and 'terrorism' while clearly presenting a security issue, is not always presented as a *cyber security* issue.

1.1 Objectives of the overall study and objective of this report

This is the second volume of a two-part study of cyber security in Albania, Bosnia and Herzegovina BiH), Kosovo*[5], Montenegro, Serbia, and The Former Yugoslav Republic of Macedonia (hereafter the WB6) assessing, in particular, how the WB6 compare in respect to the European Union's activities in this area. Volume 1 of the study focused on cyber secu-

2 Jonathon Morgan and Renee DiResta (2018), "Information Operations are a Cybersecurity Problem: Toward a New Strategic Paradigm to Combat Disinformation", *Just Security*, 10 July: https://www.justsecurity.org/59152/information-operations-cybersecurity-problem-strategic-paradigm-combat-disinformation/.

3 Schmid, A. P., & de Graaf, J. (1982). *Violence as Communication*, London, UK: SAGE Publications, p. 9.

4 Ranstorp, M. (2007). Mapping Terrorism Research. State of the Art, Gaps and Future Direction, London and New York: Routledge, pp.'s 1-2.

5 *This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo declaration of independence.

rity as traditionally or narrowly defined, so having an emphasis on cyber attacks, cybercrime, and related issues. In this volume, we take things a step further however and make the case for expanding our understanding of cyber security to encompass not just cyber attacks and cybercrime, but also cyber influence operations. These 'hard' (i.e. cyber attacks, including cybercrime) and 'soft' (i.e. 'fake news', online radicalisation, etc.) aspects of malicious cyber activity are often treated separately from each other, with attention to 'hard' issues privileged over 'soft'. The genesis of our combined approach stems from a growing awareness by the Regional Cooperation Council (RCC) that the role of the internet in information operations cannot and should not be viewed in isolation from other areas of cyber security.

The realm of cyber influence operations is murky, difficult to research and only recently receiving sustained attention from researchers, policymakers, media, and others. It is impossible to adequately treat all of its various aspects in a study of this nature. The focus in this volume is therefore on a single key example of contemporary influence operations: online radicalisation, where the internet is leveraged to gain sympathy and attract supporters for a variety of extremist and terrorist causes. This stems from an understanding, firstly, that online terrorist activity has to-date focused less on conducting cyber terrorism and more on leveraging cyber spaces and tools for other purposes, including radicalisation, recruitment, attack planning, and similar. A second practical reason for a focus on the intersections of extremism, terrorism and the Internet is that, in contrast to, for example, so-called 'fake news' and/or state-controlled social media information operations, research and analysis of the former have been underway for some time and so reliable data is available with respect to this issue, including for the WB6. This, thirdly, opens the possibility of the findings reported herein and the follow-up recommendations bearing upon other non-kinetic cyber security issues, such as those just mentioned, also.

Such an understanding on the part of the RCC has motivated them to commission this study in order to identify the linkages and overlaps between traditional narrow understandings of cyber security and a new and more expansive approach that takes 'soft' cyber security issues, such as online radicalisation, seriously. This bridging of the existing conceptual gap will, the RCC believes, assist them in implementation of their commitments in the cyber security domain, including their responsibilities in preventing and countering (online) violent extremism and terrorism. To that end, this report is divided into five sections. The first section discusses the relevant literatures, including definitional choices, and supplies a brief rundown of our methodology. The second section presents the prevalence of online extremism and radicalisation in the WB6. Section three identifies EU legislative instruments, policies, and organisations that have influenced the WB6's response and posture in this area. Section four details progress made and continuing challenges within the WB6 in respect to online radicalisation and extremism. Section five presents conclusions and recommendations.

1.2 Information Operations

Cyber security[6] is often described as the process of protecting online systems, networks, information/data and programmes from digital attack. More specifically, the EU defines it as:

[T]he safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber Security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained within.[7]

Adopted in this study however is Von Solms and Van Niekerk's (2012) much wider definition of cyber security as:

The protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace.[8]

This definition illustrates how cyber security is far more complex than just its information and/or ICT security components. It includes, in addition, the security and even wellbeing of users and the security and protection of their assets that can be accessed or reached via cyberspace. Cyber security, on this definition, stretches from protection of critical infrastructures be it international, regional, national, or local, such as the electric power grid and air traffic control systems to the security of individual internet users – such as via limiting their exposure to online bullying; cybercrime, including online fraud and extortion; 'fake news'; or online radicalisation – but while also protecting those same users' digital rights and freedoms. In terms of threat actors, hostile states, terrorists, criminals, and other malicious individuals and groups are aware that increased global digitalisation provides opportunities to them worth maximising. Targets are also many and varied. Particular threats are posed by attacks on critical infrastructure, but are not restricted to these, and can include informational attacks on elections, social cohesion, and the like.

Violent extremists and terrorists have, for some time, been utilising the internet to "communicate, collaborate and convince"[9] and it is their activities that will be concentrated on in this report. As mentioned in Vol. 1, treatment of terrorist use of the internet as a cyber security issue may seem unremarkable, excepting that it's not so-called 'cyberterrorism' that is focused on herein.

Terrorism and the internet intersect in two main ways. NATO's *Tallinn Manual* describes 'cyber terror' as "[c]yber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population".[10] The cyberterrorism threat is often portrayed via worst case scenarios, from using cyber means to shut down the electric power grid to contaminating a major water supply.[11] Every day terrorist use of the Internet, including for publicity, radicalisation, recruitment, financing, coordination, attack-planning, and a variety of other purposes, is much more commonplace however. This differentiation between cyberterrorism and terrorist use of the internet[12] is important in the context of this report for two reasons. First, the distinction goes to the heart of the issue as regards traditional narrow conceptions of cyber security, which focused on the cyberterrorism threat, while ignoring what has thus far turned out to be the greater threat: every day terrorist use of the internet. Second, there is no evidence to suggest that an incident of cyberterrorism has occurred or is imminently likely in any of the WB6, but there is ample evidence of extremist and terrorist internet use.

1.3 Online extremism and radicalisation

The concept of 'radicalisation' is highly contested,[13] but has since at least the mid-2000s taken on a negative connotation, despite the terms 'radical' and 'radicalism' continuing to be conceived of as neutral or even positive.[14] Critics of contemporary radicalisation discourse point out that 'radicalisation' has come to be associated almost exclusively with violent jihadi terrorism and is much less prevalent in discussions around other types of violent extremism and terrorism, such as the extreme right. Having said this, many countries have in the past number of years devised national-level strategies for countering radicalisation and/or violent extremism.

The impetus for development of these strategies stemmed from the 2014 emergence of the so-called 'Islamic State' (IS) and their online activity, with its heavy social media focus, which became a source of considerable anxiety for policymakers and publics globally. At the height of their online prowess in 2015, IS was producing approximately 1,200 items of official content monthly, including photo arrays, infographics, PDF magazines, and videos.[15] IS are not the only terrorists active online, of course, there are a variety of violent extremists and terrorist groups and their supporters currently engaged in a diversity of online activity.[16] A major concern is the potential connection between consumption of and networking around violent extremist and terrorist online content of whatever variety and adoption of extremist ideology or so-called 'online radical-

6 There are a very large number of definitions of cyber security available in policy documents, the academic literature, etc. It is not within the remit of this report to argue the merits or demerits of these various approaches, which would require a whole study in itself.

7 European Commission (2013). *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels: High Representative of the European Union for Foreign Affairs and Security Policy, p. 3: *http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf*.

8 Von Solms, R. and Van Niekerk, J. (2012). 'From Information Security to Cyber Security', *Computers & Security*, Vol. 39, p.101.

9 Von Behr et al. (2013), Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism, RAND Europe.

10 NATO Cooperative Cyber Defense Centre of Excellence. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press, p.104.

11 Conway, M. (2008). 'Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures.' In Dunn Cavelty, M. and Søby Kristensen, K., *Securing 'The Homeland': Critical Infrastructure, Risk and (In) Security*, London: Ashgate, pp.'s 109 – 129.

12 Conway, M. (2002). 'Reality Bytes: Cyberterrorism and Terrorist "Use" of the Internet.' *First Monday* 7(11): *http://www.firstmonday.org/issues/issue7_11/conway/index.html*.

13 Terms like radicalisation, online radicalisation, extremism, and extremist context are causally used today, with a perception of a universal understanding, but this is far from the truth. Much debate exists. This is beyond the scope of the report, but there is a wealth of literature available to explore this further.

14 Von Behr *et al*. (2013), *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, RAND Europe.

15 Winter, C. (2015). *The Virtual Caliphate: Understanding the Islamic State's Propaganda Strategy*. London: Quilliam.

16 Conway, M. (2017). 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism*, 40(1), pp.'s 82-83.

isation', with the potential to lead ultimately to engagement in 'real world' violent extremism and terrorism. Concerns have been raised, in particular, regarding easy access to large volumes of potentially influencing violent extremist and terrorist content on prominent and heavily trafficked social media platforms, including Facebook, Twitter, and YouTube, along with messaging applications, such as Telegram, Viber, and WhatsApp.

'Countering violent extremism' or CVE is the terminology used to describe activity aimed at deterring individuals from joining violent extremist or terrorist groups. CVE can take many forms, but often operates by bringing families, law enforcement, health professionals, teachers, social service employees, religious leaders, and the wider community together to dissuade individuals, particularly teens and young adults, from involvement in violent extremism or terrorism, including travel to conflict zones. Many countries globally have developed CVE strategies that seek to formalise their approach to such deterrence. Given that CVE is a relatively new concept and activity, cross-national cooperation and outreach are viewed as integral components of it, particularly for purposes of knowledge sharing and the development of best practices. This is particularly true with respect to online CVE that, due to the globe-spanning nature of the internet, must oftentimes be transnational in orientation.

1.4 Methodology

This report employed the same methodology as in Vol. 1. A mixed methods approach, which allowed for the combination of data from a variety of different sources, was adopted. The process was broken down into three phases: (i) desk-based research, (ii) field assessment and consultation, and (iii) report writing. For this volume, the desk-based research focused on extremism, terrorism, and online radicalisation.

All interviews, excepting four conducted via Skype, were carried out in the WB6 in May and June 2018. Forty-five interviews were conducted in total; all were semi-structured in nature. Of these, nine were conducted in respect to Albania, eight in Bosnia and Herzegovina, seven in Kosovo*, seven in Montenegro, seven in The Former Yugoslav Republic of Macedonia, and seven in Serbia.

To ensure inclusion of a wide breath of perspectives, stakeholders from five key fields were initially targeted: government, donor communities, the private sector, civil society, and academia. A thematic guide, based on the literature reviews, was developed for the interviews to ensure consistency across them. A combination of thematic and content analysis was then conducted. This allowed for flexibility, whilst still producing rich, detailed, and complex description of the data. A similar thematic interview model was used during all interviews. The interviews were not electronically recorded, but detailed notes were taken throughout. All interviewees were provided with a unique code to ensure anonymity, codes ranged from RB1 to RB45.

Given the scale and scope of this project, a snowballing method of sampling was used when deciding who to interview. Unlike traditional snowball sampling, where individuals interviewed nominate potential other respondents, a less traditional approach was used. If respondents raised an issue or identified an organisation that it was felt by the interviewer might be of relevance, that organisation or a similar organisation professionally tasked around the issue was contacted. For example, prosecutors interviewed highlighted gaps in training, so representatives from organisations that provide training to prosecutors and judges were later interviewed. This allowed for a broadened range of respondents to be included in the study, resulting in a more multi-disciplinary perspective.

2. PREVALENCE OF ONLINE EXTREMISM AND RADICALISATION IN THE WB6

The Western Balkans was a top European exporter of so-called 'foreign fighters' to the Syria and Iraq conflicts, with most of those joining violent jihadist organisations, such as IS and Hayat Tahrir al-Sham (and its forerunners). According to the RCC's report, *A Waiting Game: Assessing and Responding to the Threat from Returning Foreign Fighters in the Western Balkans*, approximately 1,000 individuals travelled from the Western Balkans to Syria and Iraq between the end of 2012 and the end of 2017.[17] These were largely males, including 255 males from Kosovo*, 179 males from Bosnia and Herzegovina, 79 males from Albania, 140 males from The Former Yugoslav Republic of Macedonia, 37 males from Serbia, and 18 males from Montenegro.[18] These figures make Kosovo* and BiH the top two European exporters of foreign fighters per head of population, with Albania ranked fourth, just behind Belgium.[19] This caused all of the WB6 to amend their laws to make participation in or organisation for travel to foreign conflicts illegal. This, in turn, resulted in increased arrests of those suspected of involvement in the latter types of activity.[20] A number of these fighters had prominent online presences whilst other supporters proselytised online from within the WB6. An interesting observation however is that the Internet appears to have played a lesser role in radicalisation in some WB6 economies than others.

The most prevalent types of extremist online content and activity and their impacts in each of the WB6 economies are described below. The economy case studies are not listed alphabetically in this report as they were in Vol. 1. In this section, due to

17 Azinović, V. and Bećirević, E. (2017). *A Waiting Game: Assessing and Responding to the Threat from Returning Foreign Fighters in the Western Balkan*, Regional Cooperation Council: Sarajevo: *https://www.rcc.int/download/docs/2017-11-A-Waiting-Game-29112017.pdf/e31186dab7f32945592bcbe10bd9b180.pdf*.

18 Azinović, V. and Bećirević, E. (2017). *A Waiting Game: Assessing and Responding to the Threat from Returning Foreign Fighters in the Western Balkan*, Regional Cooperation Council: Sarajevo.

19 Petrović, P. (2016). 'Islamic Radicalism in the Balkans.' *EU Institute for Security Studies (EUISS) Issue Alert* No. 24, June, p.1: *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/dsee/dv/10_balkan_radicalism/10_balkan_radicalismen.pdf*; see also Adrian Shtuni. 2015. 'Ethnic Albanian Foreign Fighters in Iraq and Syria.' *CTC Sentinel* 4(8), p.12.

20 Petrović. 2016. 'Islamic Radicalism in the Balkans,' p.2.

the focus on IS, the case study listing is based on foreign fighter numbers, from highest to lowest.

2.1 Kosovo*

IS-produced Albanian-language online content targeted Albanian speakers in Albania, Kosovo*, and The Former Yugoslav Republic of Macedonia, but with a particular focus on the Kosovo* context. In the 2014 – 2016 period, IS's overarching online narrative portrayed their so-called 'Caliphate' as a utopian destination for observant Muslims, but nonetheless requiring assistance from the *muhajirin* (i.e. emigrants) to extend, consolidate, and defend 'the state' through violence. In addition to addressing these overarching themes, IS's Albanian-language content also addressed, amongst other things, past grievances arising out of the 1998-1999 war, the alleged widespread humiliation and siege of Muslims, and rejection of the state and of mainstream Muslim clerics.[21] IS content targeting audiences in Kosovo* and Bosnia and Herzegovina generally also contained warnings that should they not embrace the "Caliphate" the horrors of the 1990s would be visited upon them again.[22] A government crackdown on jihadi foreign fighters from 2014 caused IS's Kosovar spokesmen to issue explicit warnings against those who did not share their ideology, including particularly Kosovo's* Islamic religious establishment.

Perhaps the most prominent Balkan jihadist was Lavdrim Muhaxheri (b.1987),[23] also known as Abu Abdullah al Kosovo, the self-declared "commander of Albanians in Syria and Iraq." Muhaxheri travelled to the region in 2012 to join the al-Qaeda affiliated Jabhat al-Nusra, but later sided with IS. He was notorious in the Balkans for a 2014 video in which he can be seen beheading a man accused by IS of spying for the Iraqi government and a 2015 video in which he is shown killing a man with a rocket-propelled grenade.[24] Prior to these, Muhaxheri also featured in one of the first videos to emerge of the Kosovo* Albanian foreign fighter contingent in Syria. The November 2013 video shows an armed Muhaxheri, with two tanks in the background, speaking of victory for IS, a land without *kufrs* (i.e. unbelievers), and appealing to Kosovars to join the *jihad*.[25] Muhaxheri is reported as having died in Syria, allegedly in a US airstrike, in June 2017.[26]

Another prominent Kosovar IS member was Muhaxheri's close associate Ridvan Aqifi (b.1990), also known as Ridvan Haqifi, Ridvan al-Albani, and by the *kunya* or *nom de guerre* Abu Muqatil. In November 2014, Kosovars were shocked by Aqifi's call for the murder of those who had helped retrieve a young Kosovar boy after his jihadi father abducted him and took him to Syria.[27] Between 4 and 16 November 2016, eighteen Kosovo* Albanians and one Albanian from The Former Yugoslav Republic of Macedonia were arrested for plotting terrorist attacks in Kosovo* and Albanian. Together with Muhaxheri, Aqifi is thought to have coordinated the group of ethnic Albanians who plotted to carry out a series of attacks, including on the Israeli soccer team during a match in Albania. Aqifi is thought to have been killed in Syria in February 2017.

Both Muhaxheri and Aqifi featured in the fourth instalment of IS's *Clanging of the Swords* video series. Released by IS's Al-Furqan media outlet in May 2014, *Clanging of the Swords, Part 4* is just over one hour in length, and was clearly meant as a warning to IS's enemies, far and near, that it was – to utilise its own terminology – "remaining and expanding". Muhaxheri can be seen from two minutes into the video delivering a speech in Arabic surrounded by a crowd of other IS fighters, including Aqifi, many of whom are holding passports that they later set alight. Muhaxheri grips his Kosovo* passport in his left hand and a short sword in his right while speaking, until such time as he rips up the passport, throws it on the ground, stamps on it with his booted foot, and declares it "a passport of *kufars*."[28] The Kosovar's prominent display of his passport is "not accidental," says Kraja, "the long-awaited passport of the young nation meant to elicit pride among its citizens is thrown on the ground, stomped on and burned in a sign of defiance to the secular state as a product of Western intervention."[29]

21 Garentina Kraja. 2017. *The Islamic State Narrative in Kosovo: Deconstructed One Story at a Time*. Pristina: Kosov-* Centre for Security Studies, p.24.

22 Kraja. 2017. *The Islamic State Narrative in Kosovo*, p.20. For example, approximately ten minutes into the video 'Honor is in the Jihad: A Message to the People of the Balkans' a speaker says, "Srebrenica will be repeated again. The massacres in Gorazde, Mostar, and other places will be repeated again, if the Muslims don't return to their religion."

23 American Foreign Policy Council. 2017. *The World Almanac of Islamism 2017*. Lanham, MD: Rowman and Littlefield, p.573.

24 Jack Moore. 2017. 'Who is Lavdrim Muhaxheri? ISIS Balkans Commander, Architect of Israel World Cup Plot, Now Dead.' *Newsweek*, 8 June.

25 Kraja. 2017. *The Islamic State Narrative in Kosovo*, p.24.

26 Moore. 2017. 'Who is Lavdrim Muhaxheri?' Though it is worth pointing out that Muhaxheri was erroneously reported as dead on a previous occasion in August 2014; see Joanna Paraszczuk. 2015. '"Dead" Kosovar Albanian IS Militant Resurfaces In Gruesome Killing Video.' *RFE/RL*, 26 May.

27 Paraszczuk. 2015. '"Dead" Kosovar Albanian IS Militant Resurfaces.'

28 A copy of *Clanging of the Swords, Part 4*, with English subtitles, may be accessed at *https://jihadology.net/?s=clanging+of+the+swords+part+4*.

29 Kraja. 2017. *The Islamic State Narrative in Kosovo*, p.27.

An exemplary example of IS messaging targeting Albanian speakers was the 20-minute long June 2015 al-Hayat video entitled 'Honor is in the Jihad: A Message to the People of the Balkans.' A criticism of the video made by Kraja is that "[i]t tends to lump together Kosovo* with Bosnia—despite their stark differences—in appealing to these two [economies] religious identities and histories as [economies] that were once part of the Ottoman Empire, but also the shared history and the memory of the 1990s wars."[30] At least 11 men and three small children appear in the video, with eight of the men speaking on camera in various Balkan languages and dialects. Of the latter, five are identified as Bosnian, two as Albanian, and just one as Kosovar. The Kosovar appears to be Ridvan Aqifi who about three-quarters of the way through the recording states:

By Allah, black days are coming to you. By Allah, you will fear to walk in the streets. You will fear working in your offices. You will fear. You will be terrorised and feel depressed even in your homes. We will put fear in you and terrorise you even in your dreams when you are asleep…We will kill you with the permission of Allah. We will come to you with explosive belts.[31]

This is in keeping with the shift from early content targeted at Albanian-speaking audiences emphasising *hijra* (i.e. migration) to a post-2014 emphasis on threats and calls for supporters to carry out attacks in their home economies.[32] This mirrors a shift that took place in the broader IS narrative, in whatever language, albeit this broader shift from a focus on migration to the 'Caliphate' to carrying out independent acts of terrorism at home occurred later, from about 2015.

While direct personal contact with IS recruiters was underlined by Garentina Kraja "as a crucial factor in the process of Radicalisation" for some Kosovars, she emphasises that social media, "especially videos on YouTube," also played a role.[33] In particular, Kraja mentions two Kosovars who had contact with IS recruiters who played online content for them in face-to-face settings, which they described as instrumental in their radicalisation processes. In police interviews, one defendant who had known Lavdrim Muhaxheri since his teenage years described meeting him on at least two occasions before he departed for Syria; both times Muhaxheri played him "videos and similar material on YouTube of killings and rapes" allegedly taking place in Syria. That "and his appeal through electronic media in 2013 where he openly calls on the young in Kosovo* to join the holy war in Syria," the defendant claimed played a role in the defendant's own decision to join IS. Another defendant described his radicalisation similarly, explaining how he was exposed to the Syria conflict by Ridvan Aqifi: "He would come to the gym near the car wash I ran and he would stop and talk to me in particular about the war in Syria. He would show me videos of the war in Syria and would invite me to go and fight there."[34]

In addition to highlighting the role of social media, a number of reports on IS-related activity in Kosovo* mention the part played by traditional mass media in radicalisation and recruitment processes. "Social media, especially videos disseminated through YouTube but also through the unfiltered transmission of their messages in Kosovo's* mainstream media, are vital to recruitment efforts of IS in Kosovo*," Kraja wrote.[35] Kosovo's* television stations became, in effect, "the very vehicles of the dissemination of their propaganda." Her explanation for this is the pressure of 24-hour news cycles. She is nonetheless very critical of the unfiltered broadcasting of IS videos, in particular "their full availability on their [TV station's] websites [that] unintentionally turned mainstream media, which in Kosovo* have hundreds of thousands of followers, into platforms from which IS continued to spread its propaganda unhindered."[36]

2.2 Bosnia and Herzegovina

As already mentioned, of the eight men who speak on camera in the 2015 al-Hayat-produced video 'Honor is in the Jihad: A Message to the People of the Balkans,' five are identified as Bosnian. Just shy of four minutes into the production, a man identified as Salahuddin al-Bosni advises "If it is that hard for you and you want it so much, then make *Hijrah*." This was a standard component of the IS narrative in 2014 and 2015. Nearly five minutes into the video the same speaker also advises:

If you can, put explosives under their cars, in their houses, all over them. If you can, take poison and put in their meal or in their drink. Make them die, make them die of poisoning. Kill them wherever you are. In Bosnia, in Serbia, in Sandzâk.[37] You can do it. [38]

30 Kraja. 2017. *The Islamic State Narrative in Kosovo**, p.21.

31 Also quoted in Kraja. 2017. *The Islamic State Narrative in Kosovo**, p.30.

32 Kraja. 2017. *The Islamic State Narrative in Kosovo**, p. 24.

33 Kraja. 2017. *The Islamic State Narrative in Kosovo**, p.31.

34 Kraja. 2017. *The Islamic State Narrative in Kosovo**, p.32.

35 Kraja. 2017. *The Islamic State Narrative in Kosovo**, p.7.

36 Kraja. 2017. *The Islamic State Narrative in Kosovo*, p.34.

37 Sandžak or Sanjak is a historical geo-political region, a former Ottoman administrative district, in the Serbia and Montenegro border regions.

38 Sandžak or Sanjak is the name sometimes used to describe the Serbia-Montenegro border region.

Again, this was standard online advice to IS followers, especially from 2015 onward. Despite the prominence of Bosnians in the above video, at least one recent analysis points to 'real world' contacts in families and communities, including via Salafi citizens' associations, as the main radicalisation route in Bosnia and Herzegovina.[39] Acknowledged however is that certain communities, such as disenfranchised youth, "may face a unique vulnerability to Internet-based recruitment."[40] Two particular aspects of the internet underlined by Bećirević in her work on extremism and radicalisation in BiH are, first, the fact that much Salafi online activity falls into the category of legitimate religious discussion and, second, the transnational character of a large portion of extremist activity.

The majority of Salafis are non-violent and so a significant portion of Salafi's online activity is protected religious discussion. This throws-up difficulties for researchers, the authorities, and others interested in monitoring online violent extremist activity however, as distinguishing between violent and non-violent radicalism can be challenging, with some ideologues being careful to adopt rhetoric that carefully avoids falling into the violent extremism category and others drifting back and forth across this line. As regards the latter, Bećirević supplies the example of a 2016 online video, which featured ISIS-type imagery overlaid with audio of a 1999 lecture by Safet Kuduzović in which he called for violence against Jews, the deaths of people who curse the Prophet, and said that non-Salafi Muslims "deserve nothing else but to be killed".[41] Kuduzović, who claims not to be a supporter of violent jihadi ideology, took over as head of BiH's Salafi community in the wake of its previous leader, Nusret Imamović,[42] departing for Syria in 2015, and another being jailed for recruiting for IS.[43] According to Bećirević, this video caused many Bosnians to question whether there was any true difference between ultra-conservative Salafis and advocates of violent extremism.[44]

At time of writing (September 2018), Safet Kuduzović has just over 25,700 followers on Facebook.[45] His page is updated approximately weekly with videos of his lectures, with numbers of views for recent uploads ranging from 4,000 to 7,000. Kuduzović does not interact with his Facebook 'friends'; he uses the platform for broadcast purposes only. More prominent online than Kuduzović is his mentee, Elvedin Pezić. Pezić's Facebook page, on which he generally posts multiple times daily, has over 123,000 followers.[46] Recently uploaded videos by Pezić have garnered between 20,000 and over 40,000 views. His posts generally address appropriate conduct for Salafi religious adherents living in a non-Salafi society, including making recommendations to, for example, avoid music concerts, dress conservatively, and promoting female marital obedience. Unlike Kuduzović, Pezić also takes the social element of 'social media' seriously, responding to commenters, engaging in discussion, and re-posting other users' content, thus conveying that "he is available, open, and has time to attend to his brothers and sisters in faith."[47] Like Kuduzović, Pezić's videos are also widely available on YouTube and Vimeo.

The Internet is widely recognised as having facilitated the establishment and spread of a wide variety of transnational networks, including Salafi and jihadi networks. There is a large Bosnian diaspora, with notable Salafi contingents in Austria, Germany, the Netherlands, Slovenia, and Sweden, which are now connected via the Internet. Mentioned by Bećirević, and discernible from a variety of Facebook pages, is that Salafi lectures and events across BiH are highly coordinated. Bosnia and Herzegovina is also a component in a broader Europe-wide lecture circuit and:

Many of the key figures on this circuit stream and post videos of their lectures online, employing rhetoric that is at times even more extreme than that of Pezić or Kuduzović. Among these ideologues, the most influential in BiH has been Vienna-born *takfiri* ideologist Nedžad Balkan, known as Abu Muhammed. Before his arrest by Austrian police in early 2017, Balkan had preached among the most extreme interpretations of *takfirism* (particularly targeting and condemning Muslims who do not adhere to Salafism). He is a hero of violent factions of the Salafi movement in BiH, Montenegro, and the Sandžak.[48]

Given the nature of the Internet, in other words, there was no requirement for Balkan to actually be in the Balkans to influence users there. As in Kosovo*, the combination of 'real world' and online overlaps is worth noting here too.

A role for the internet in the increased nationalist rhetoric apparent in Bosnia and Herzegovina has also been mooted. This too is often driven by users and groups outside of the jurisdiction. In 2017, BIRN located more than 60 websites based in the Western Balkans "promoting the idea of ethnically pure nation states, neo-Nazism, violent homophobia and other radical right-wing policies."[49] These were described as established and maintained by a new generation of region-wide extremists "even more radical than those who split up the former Yugoslavia."[50] In terms of the groups and sites analysed by BIRN, most had links to similar groups Europe-wide and "all agree on wanting a piece of Bosnia."[51] The latter is not just a common theme of Croat and Serb nationalists, but also some radical Islamist groups.[52] While most Bosniak far right groups are linked to radical Islamism, at least one group has emerged advocating a secular Bosniak state, while at the same time naming Jews, Roma, Communists, the LGBTQ+ community, and non-whites as enemies of Bosnia. According to BIRN, the moderator of this group's website is from Sarajevo, but now lives in Sweden, and posts under the screen name of a former Balkan SS officer.[53]

2.3 Albania

As already discussed with regard to Kosovo*, there is considerable pro-IS Albanian language content available online. Already mentioned too was that the Albanian authorities foiled an attack on the Israeli soccer team ahead of a match against Albania in the northern Albanian town of Shkoder, which was said to have been masterminded by the Kosovar IS leader, Muhaxheri. While it appears that the Internet played a significant part in Kosovar foreign fighters' radicalisation processes, but that community ties and face-to-face contacts were more consequential in the case of BiH, there is some disagreement as to the role of online in radicalisation in Albania. "Transnational cooperation of violent extremists according to some of the key informants is present sporadically within the Albanian-speaking communities in the Balkans, most notably between Albania, Kosovo* and [The Former Yugoslav Republic of] Macedonia"[54] This Albanian language connection is underlined to a much greater extent by researchers and some media however. The latter identify greater transnational connections, which they put down at least partially to the borderless nature of the Internet, which they view as a crucial contemporary influence channel. One academic stated in an interview that "[t]ransnational cooperation surely occurs, even at this moment online or in-person. The online influences in a way or another are present and take place also among religious believers [everyone has access to online content beyond borders]."[55] The report's author, Gjergji Vurmo, rightly point out that this is more of a function of the transnational influence of online terrorist content, due to its wide dissemination via a multiplicity of online platforms, rather than transnational cooperation between violent extremist groups *per se*.[56]

Vurmo's concern is that "offline peer to peer radicalisation seems to be underestimated" in Albania.[57] Zhilla, an academic, has suggested that "a considerable number of young Albanians, especially those with little religious knowledge, are approaching

39 Edina Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*. London: British Council, p.4. See also, for example, Igor Spaic. 2015. 'Bosnia: Salafist Leader Gets Seven Years for Recruiting Boys to Islamic State.' *Organized Crime and Corruption Reporting Project (OCCRP)* 6 November: *https://www.occrp.org/en/blog/4579-bilal-bosnic-salafist-leader-gets-seven-years-for-recruiting-boys-to-islamic-state*.

40 Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, p.4.

41 Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, pp.'s 18 – 19.

42 Imamović was listed by the UN Security Council on 29 February 2016, pursuant to paragraphs 2 and 4 of resolution 2161 (2014), as being associated with Al-Qaida. The listing also states that "Before departing for Syrian Arab Republic, Imamovic was accused of recruiting many citizens of Bosnia and Herzegovina to fight for the Al-Nusrah Front." See *https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list/summaries/individual/nusret-imamovic*.

43 Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, p.19; Spaic. 2015. 'Bosnia: Salafist Leader Gets Seven Years for Recruiting Boys to Islamic State.'

44 Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, p.18.

45 This is a notable increase in followers (i.e. approx. 5,000) compared to that reported in Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, p.19. Worth noting is that both sets of figures refer to Kuduzović's 'Public figure' profile at *https://www.facebook.com/Safet-Kuduzovi%C4%87-1819196525023053/*. Kuduzović also has an 'Education website' at *https://www.facebook.com/drsafetkuduzovic/*.

46See *https://www.facebook.com/pezicelvedin/*. This is, like for Kuduzović, a significant increase on the 82,000 followers reported in Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, p.19.

47 Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, p.19.

48 Bećirević. 2018. Extremism Research Forum: Bosnia and Herzegovina Report, p.19.

49 Marija Ristic, Sven Milekic, Maja Zivanovic, Denis Dzidic. 2017. 'Far-Right Balkan Groups Flourish on the Net.' Balkan Insight 5 May: *http://www.balkaninsight.com/en/article/far-rightbalkan-groups-flourish-on-the-net-05-03-2017*.

50 Ristic *et al*. 2017. 'Far-Right Balkan Groups Flourish on the Net.'

51 Ristic *et al*. 2017. 'Far-Right Balkan Groups Flourish on the Net.'

52 Ristic *et al*. 2017. 'Far-Right Balkan Groups Flourish on the Net.' See also Bećirević. 2018. *Extremism Research Forum: Bosnia and Herzegovina Report*, pp.'s 41 – 42.

53 Ristic *et al*. 2017. 'Far-Right Balkan Groups Flourish on the Net.'

54 Gjergji Vurmo. 2018. *Extremism Research Forum: Albania Report*. London: British Council, p.23.

55 Vurmo. 2018. *Extremism Research Forum: Albania Report*, p.23.

56 Vurmo. 2018. *Extremism Research Forum: Albania Report*, p.25.

57 Vurmo. 2018. *Extremism Research Forum: Albania Report*, p.25.

ISIS propaganda through social media such as Facebook."[58] A Mufti from the Albanian Muslim Community told an interviewer that, in his opinion, dissemination of extremist messaging took place through direct communication about 70% of the time and about 30% via the Internet.[59] A separate Albanian Muslim Community official insisted, on the other hand, that "[t]he first contact to this ideology is not through internet but peer-to-peer, social media is not the most important way of dissemination in Albania."[60] This seems to be borne out in an article by Shtuni on Albanian foreign fighters covering the period 2012 to 2015, which contains no mention of relevant online activity.[61] Shtuni does point out however that the age group most susceptible to recruitment as foreign fighters in the Albania case was 31 to 35 years;[62] they skew slightly older than was the case for some other economies in other words and so may not have been as heavy social media users. As regards the role of the internet in Albanian jihadis' radicalisation therefore, consensus on the part of academics and Muslim community leaders, at least, seems to be that while the Internet has a role to play, face-to-face contacts are still paramount.

2.4 The Former Yugoslav Republic of Macedonia

While none of the speakers in the June 2015 IS video targeting a Balkan audience has a *kunya* identifying himself as from The Former Yugoslav Republic of Macedonia, a passport of The Former Yugoslav Republic of Macedonia is one of those shown being torn up. 'Honor is in the Jihad' was not the only IS-related online activity. At least two returned foreign fighters from The Former Yugoslav Republic of Macedonia prosecuted under Article 322-A of The Former Yugoslav Republic of Macedonia's criminal code had online presences. Fazli Sulja (23) and Muhamed Shehu (27) were each sentenced to five years in prison for participating in foreign paramilitary organisations; both had uploaded photographs depicting their involvement in the Syria conflict to their social media profiles.[63]

A consistent finding in interviews carried out for a 2018 report focused on extremism in The Former Yugoslav Republic of Macedonia was easy access to extremist and terrorist content via the Internet, especially social media. As one high school teacher observed, "there are enough convincing materials … especially it is the case with videos and violent content." Another teacher felt that young users searching for these materials had insufficient understanding of the potentially very serious real world implications of their viewing: "they said that they feel it as a film."[64] The long shelf life of radical and extremist content is underlined in the same report:

> Additionally, once radical content is created, its shelf life on the internet sometimes even outlives its creators. For example, despite the fact that Rexhep Memishi has now been jailed as a result of the Cell operations, his YouTube channel "Minber Media" was still being uploaded with new content well after his incarceration, and has over 7 million views. Similarly, his "Minber Media" Facebook page with 54,000 "likes" continues to be active to this day, with weekly updates of new content.[65]

A concern for the report's authors is that despite Memishi's imprisonment, online content produced by and/or featuring him lends his extremist narrative continuity and thus his "digital legacy" has the potential to continue to negatively influence people from The Former Yugoslav Republic of Macedonia (and other Albanian speakers).[66] This has certainly been shown to be the case with respect to high profile violent jihadi ideologues, such as Anwar al-Awlaki, who had significant online presences prior to their deaths that have continued to influence adherents long after.[67]

2.5 Serbia

The findings of a public opinion survey conducted among young people from Sandžak showed that more than half of respondents (52.6%) viewed online platforms as crucial for dissemination of extremist views and content. Almost half of respondents (46.7%) to the same survey thought that, in terms of online dissemination, social media platforms were the most important tool for extremist propaganda. Considerably lower numbers of respondents felt that important for the spread of extremist messaging were "religious objects" (7.1%) or that such messaging was widespread "in the community" (8.3%).[68] The report's authors believe "[t]his finding indicates the importance of [the] internet as a channel of dissemination of extremist messages."[69]

In terms of jihadis, and as already discussed, connections among them are often predicated on shared languages. The implication of this is that Serbian jihadis are most closely connected to those from Bosnia and Herzegovina and Montenegro. There is some cooperation with Kosovo*, according to Petrović and Stakić, but this is rare because it depends upon older Kosovars who speak Serbian/Bosnian.[70] The latter are less likely than their younger cohorts to be heavy and accomplished Internet users and thus a significant role for the Internet in these exchanges seems relatively unlikely. Where technology does play a significant part according to a recent report on jihadi extremism in Serbia is with regards to visits of extremists from elsewhere for purposes of in-person sermons, lectures, and similar:

> I saw that they are using conference videos for broadcasting their meetings and discussions to other masjids, even to other states. This communication goes in both directions. For this reason, field visits of the leaders from other countries are not as important as they used to be in the past.[71]

This is in keeping with findings from elsewhere in the region, including Kosovo*[72] and Montenegro.[73] It also segues very well with what is happening in Serbia's extreme right online scene.

If, of the WB6, Kosovo* has received most attention from scholars, policymakers, and media regarding the use of the Internet in Kosovar jihadi radicalisation processes, Serbia has received not equal but nonetheless considerable attention to its online extreme right scene. Interviewees monitoring this area reported a growing right wing sentiment both online and off-line, which has increased as the number of migrants has increased, or at least the amount of media coverage and political attention being given to migrants has increased. The transnational connections within this extreme right online scene are worth commenting upon here.

In 2017, BIRN located 30-plus Serbian-language extreme right websites. Generally, according to Ristić *et al.*, these sites "deny or denounce the independence of Kosovo*, demand the union of all Serbian people in one state, denounce the EU and champion Christian Orthodox Russia." Most of them are also strong supporters of Russian actions in Ukraine, particularly its seizure of Crimea. In January 2017, for example, Aleksandar Djurdjev, the leader of the Serbian League, registered the URL Srpska.tv. Djurdjev has been critical of the Serbian press, which he says is among other things too pro-EU and unwelcoming of contrary opinions. "The internet as a multimedia media, with all its possibilities, has become our dominant channel of communication," he said. In February 2017, Srpska.tv posted a video about a mural being painted by activists from the Serbian League and allied groups heralding a Russian commander killed in eastern Ukraine. In terms of neo-Nazism, the leader of the National Machine, Goran Davidovic, is, along with another member of his group, being tried in absentia in Serbia for initiating national, racial, and religious hate and intolerance. Despite being wanted by Serbian authorities, Davidovic, who now lives in Italy, continues to maintain a presence in Serbia via his personal website and social media profiles.[74]

2.6 Montenegro

When asked, for a recent report, about forms of extremism in Montenegro, interviewees identified three main types: violent *takfirism* (termed in this report 'violent jihadism'), non-violent Salafism, and pan-Slavism and Orthodox extremism. In terms of the latter type, some Montenegrins have joined the foreign fighter contingent in eastern Ukraine.[75] As regards the former, according to an imam from the official Islamic Community of Montenegro (ICM), 'real world' evangelisation by both violent and non-violent Islamist extremists is in decline in the economy; "both…have moved their activities to the Internet," he told an interviewer.[76] Other interviewees, including intelligence officials and others who monitor social media and have engaged with some radicalised youth and their families, linked some cases of radicalisation into non-violent extremism

58 Aleksandra Bogdani, 2016. 'Albania Faces the Risk of Shadow Jihadi Warriors.' *BIRN*, 26 March: https://www.reporter.al/shqiperia-perballet-me-rrezikun-e-luftetareve-xhihadiste-ne-hije/.

59 Vurmo. 2018. *Extremism Research Forum: Albania Report*, p.13.

60 Vurmo. 2018. Extremism Research Forum: Albania Report, p.14.

61 Adrian Shtuni. 2015. 'Ethnic Albanian Foreign Fighters in Iraq and Syria.' CTC Sentinel 8(4).

62 Shtuni. 2015. 'Ethnic Albanian Foreign Fighters,' p.14.

63 Stojkovski and Kalajdziovski. 2018. *Extremism Research Forum: Macedonia Report*, p.36.

64 Stojkovski and Kalajdziovski. 2018. *Extremism Research Forum: Macedonia Report*, p.19.

65 Stojkovski and Kalajdziovski. 2018. *Extremism Research Forum: Macedonia Report*, pp.'s 19 – 20.

66 Stojkovski and Kalajdziovski. 2018. *Extremism Research Forum: Macedonia Report*, p.20.

67 Donald Holbrook. 2017. *What Types of Media Do Terrorists Collect? An Analysis of Religious, Political, and Ideological Publications Found in Terrorism Investigations in the UK*. The Hague: ICCT.

68 Predrag Petrović and Isidora Stakić. 2018. *Extremism Research Forum: Serbia Report*. London: British Council, p.15.

69 Petrović and Stakić. 2018. *Extremism Research Forum: Serbia Report*, p.15.

70 Petrović and Stakić. 2018. *Extremism Research Forum: Serbia Report*, p.30.

71 Petrović and Stakić. 2018. *Extremism Research Forum: Serbia Report*, p.15 and p.30.

72 See section 2 of this report.

73 See section 4 of this report.

74 Ristic *et al*. 2017. 'Far-Right Balkan Groups Flourish on the Net.'

75 Bećirević et al. 2018. Extremism Research Forum: Montenegro Report, p.3.

76 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.9; see also p.19.

to online activity and influences.[77] According to one journalist, for example:

Salafists have not been as active as they used to be in organising lectures, but even occasional events are enough to initiate new adherents. Then, they have a vast online Salafi community to turn to in order to maintain their beliefs. Preachers from Bosnia are especially popular among youth. They used to come and lecture more in person, but lately they are more reliant on online lectures. Preachers such as Safet Kuduzović and Elvedin Pezić stream their lectures live, and people watch these instead of official Islamic Community lectures.[78]

Pezić is said to have a particular appeal to youth, both because he is humorous and intentionally directs his message toward a youth audience. Edina Bećirević and her team found that in November 2017 Kuduzović had 700 Montenegrin followers, accounting for just 3% of his total follower count and Pezić had 2,164 Montenegrin followers, constituting less than 2.5% of his following.[79] Pointed out too was that Montenegro lacks a charismatic domestic jihadi or non-violent Salafi leader, with or without an online presence.[80] Numerous of Bećirević *et al.*'s interviewees referred to Hafiz Sulejman Bugari, formerly an imam in the official BiH Islamic Community and a recent transplant to Montenegro, as swiftly gaining a high profile and a diversity of adherents, and having a moderating influence. Interestingly, Bugari, who is a Sufi, is alleged to have departed Sarajevo due to intense online trolling he was exposed to by Salafi preachers and their followers in Bosnia and Herzegovina. Certainly, Bugari has been widely attacked by Salafis in lectures and online posts for *bidah* or heresy, and for "spoiling Muslim youth with his poisonous teachings." According to one interviewee, "unlike domestic Salafi preachers, [Bugari] is very charismatic and popular. Plus, he is constantly in contact with young people and is social media savvy." As the report's authors call attention to, Bugari's prominence is:

[A] reminder that the role of a charismatic leader in religious proselytism can sometimes be even more important than dogma…The example of Bugari, who has managed to offer a serious alternative to the Salafi narrative in only a couple of months of working with the ICM and lecturing throughout Montenegro, demonstrates how little it may take for alternative narratives to effectively take hold.[81]

2.7 Summing-up

Apart from the borderless nature of the internet generally, there is also an important transnational dimension to much of the extremist online content and activity in the WB6 region, due to factors such as shared languages, key influencers, and diaspora links. While the role of the internet in radicalisation processes is evident to a greater or lesser extent across the WB6, personal interactions are no less important. In fact, in some economies, the latter are viewed as a more important factor. Also worth underlining is that, although the substance of the content differs, similar online practices are identifiable across ideologies albeit considerably more attention from researchers, policymakers, and media has been directed to Islamist extremist, particularly violent jihadi online content and activity than any other variety apparent in the WB6.

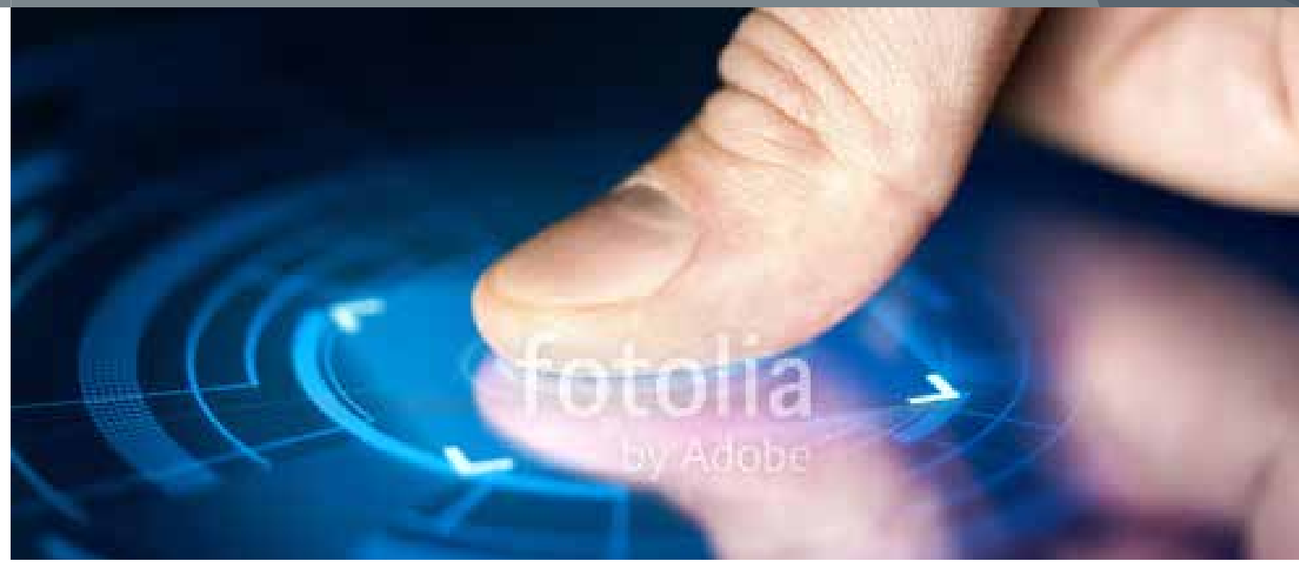
77 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, pp.'s 9 - 10.

78 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.13.

79 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, pp.'s 13 – 14. It should be noted that these counts have probably increased, perhaps substantially, in 2018, given the increased Facebook follower counts recorded for both Kuduzović and Pezić in this report.

80 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.14.

81 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.22.



3. EUROPEAN AND INTERNATIONAL ENVIRONMENTS

This report supplies an overview of the situation in the WB6 with respect to the intersections of violent extremism, terrorism, and the Internet, with a particular focus on online radicalisation. Also at issue, as in Vol. 1, is what is driving WB6 government activity in this area, especially with regard to legislation, strategies, and policies, with a specific emphasis on the influence of EU activity, but also taking into account other relevant actors and initiatives. Interestingly, and unlike while conducting the field research in relation to traditional cyber security issues, there was little reference to specific activities conducted by the EU and other organisations in the area of online radicalisation, excepting programmes and projects that directly impacted the WB6. Instead, the impetus for progress in this area appeared to be the recognition that individual economies and the region as a whole faced 'real world' risks from violent extremism and terrorism, including its online components, and thus these issues could not be left unaddressed.

Leaving interview data aside however, it is clear that WB6 government activity in this area, including legislation, response strategies, and other policies has been considerably influenced by the EU's counter-terrorism policies and practices, including with respect to the internet. These include the European Union Counter-Terrorism Strategy, the EU Strategy for Combating Radicalisation and Recruitment, the Joint Action Plan on Counter-Terrorism for the Western Balkans to be signed on behalf of the EU with Western Balkans Partners, the EU Counter Terrorism Directive, the European Union Internet Forum (EUIF), the EU Internet Referral Unit (EU IRU), and the EU's Radicalisation Awareness Network (RAN). Of relevance too are strategies and/or activities addressing online radicalisation and related issues devised by the Organization for Security and Co-operation in Europe (OSCE), the Council of Europe, the Global Internet Forum to Counter Terrorism (GIF-CT), the United Nations Counterterrorism Executive Directorate (UNCTED), and NATO. Each of these is treated individually below in order to supply context for the WB6's posture on online radicalisation and responses to it, which will be discussed in section 4.

3.1 European policy documents and strategies

3.1.1 The European Union Counter-Terrorism Strategy

The EU published its Counter-Terrorism Strategy in 2005 as part of its "strategic commitment: To

combat terrorism globally while respecting human rights, and make Europe safer, allowing its citizens to live in an area of freedom, security and justice".[82] The strategy is composed of four major work strands, under the headings Prevent, Protect, Pursue, and Respond,[83] which are explained as follows:

PREVENT: To prevent people turning to terrorism by tackling the factors or root causes which can lead to radicalisation and recruitment, in Europe and internationally;

PROTECT: To protect citizens and infrastructure and reduce our vulnerability to attack, including through improved security of borders, transport and critical infrastructure;

PURSUE: To pursue and investigate terrorists across our borders and globally; to impede planning, travel and communications; to disrupt support networks; to cut off funding and access to attack materials, and bring terrorists to justice;

RESPOND: To prepare ourselves, in the spirit of solidarity, to manage and minimise the consequences of a terrorist attack, by improving capabilities to deal with: the aftermath; the coordination of the response; and the needs of victims.[84]

While the strategy acknowledges that the primary responsibility for combatting terrorism rests with Member States, it sets out how the EU can add value in this area. Four key ways of doing this are identified: (i) strengthening national capabilities, (ii) facilitating European cooperation, (iii) developing collective capability, and (iv) promoting international partnership.[85] The strategy explicitly refers to combatting radicalisation and recruitment, including "identify[ing] and countering the methods, propaganda and conditions through which people are drawn into terrorism".[86] With regards to the internet specifically, paragraph 9 of the Prevent section of the strategy states:

There are practical steps an individual must take to become involved in terrorism. The ability to put ideas into action has been greatly enhanced by globalisation: ease of travel, transfer of money and communication—including through the internet—mean easier access to radical ideas and training. We need to spot such behaviour…We also need to disrupt such behaviour by: limiting the activities of those playing a role in radicalisation; preventing access to terrorist training; establishing a strong legal framework to prevent incitement and recruitment; and examining ways to impede terrorist recruitment through the internet.[87]

In addition, a list of seven key priorities for the Prevent pillar are supplied, the top one of which is to "develop common approaches to spot and tackle common behaviour, in particular the misuse of the internet".[88] The internet is also briefly mentioned in the strategy's Pursue section where it is stated that terrorists "must also be deprived as far as possible of the opportunities offered by the Internet [*sic*] to communicate and spread technical expertise related to terrorism".[89]

While *The European Union Counter-Terrorism Strategy* has not been updated since 2005, a *Strategy for Combating Radicalisation and Recruitment to Terrorism* also appeared first in 2005, but has been updated multiple times since. [90]

3.1.2 EU Strategy for Combating Radicalisation and Recruitment to Terrorism

The EU's *Strategy for Combating Radicalisation and Recruitment to Terrorism* was first published in November 2005,[91] with updates in 2008 and 2014. The main objective of the 2014 version of the strategy is, for example, "to prevent people from becoming radicalised, being radicalised and being recruited to terrorism and to prevent a new generation of terrorists from emerging".[92]

Right from the outset, this strategy – the first version of which appeared a month before the overall counter-terrorism strategy – had an emphasis on "disrupting the activities of the networks and individuals who draw people into terrorism". In fact, the 2005 *Strategy for Combating Radicalisation and Recruitment to Terrorism* uses very similar language to that used in the Prevent section of *The European Union Counter-Terrorism Strategy* to describe the role of the internet in terrorism:

There are practical steps an individual must take to become involved in terrorism. The ability to put ideas into action has been greatly enhanced by globalisation: ease of travel and communication and easy transfer of money mean easier access to radical ideas and training. The internet assists this facilitation and provides a means for post-attack justification.[93]

In terms of responses, the strategy advocates "effective monitoring of the Internet" and "examin[ation] of ways to impede terrorist recruitment using the Internet". It also pledges to "pursue political dialogue and target technical assistance to help others outside the EU to do the same".[94]

While the internet is not mentioned specifically, paragraph 10 of the 2005 *Strategy for Combating Radicalisation and Recruitment* is also worth quoting given its emphasis on extremist propaganda and its effects:

There is propagation of a particular extremist worldwide which brings individuals to consider and justify violence. The core of the issue is propaganda which distorts conflicts around the world as a supposed proof of a clash between the West and Islam and which claims to give individuals both an explanation for grievances and an outlet for their anger. This diagnosis distorts perceptions of Western policies and increases suspicious of hidden agendas and double standards.[95]

Similar sentiments are expressed in the 2014 revision of the Strategy.[96]

The latest version of the strategy (i.e. 2014) also notes the need to:

Acknowledge that the means and patterns of radicalisation and terrorism are constantly evolving. Home grown terrorists, individuals supporting extremist ideology linked to terrorism, lone actors, foreign fighters and any other form of terrorism, as well as the mobilisation and communication potential of the Internet and social media present possible channels through which radicalisation and recruitment to terrorism could occur.[97]

To ensure effective action and implementations of the Strategy's aims and objectives, it therefore advocates the necessity of consistently revisiting priorities in order to ensure that the EU's "security approach can address emerging forms of threats".[98] Such consistent revisiting has particular importance with respect to online radicalisation, as both the internet and extremist landscapes are both very fast changing. Whilst not mentioning the internet *per se*, the revised Strategy also emphasises the importance of cooperation, including with the private sector:

Overall, the challenge of radicalisation and recruitment to terrorism will not be met by governments working alone, but by collaboration with communities, civil society, nongovernmental organisations (NGO) and the private sector. It requires a joint effort at local, regional, national, European and international level.[99]

82 Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*. Brussels: Presidency and CT Coordinator, European Council, p. 2: *https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204*.

83 It is worth noting here that the UK, holding the EU Presidency for the second half of 2005, drafted what ultimately became the European Union Counter-Terrorism Strategy in December 2005, which was directly based on the UK's own counter-terrorism strategy, including having the same four pillars. See Wensink, W., Warmenhoven, B., Haasnoot, R., Wesselink, R., Van Ginkel, B., Wittendorp, S., Paulussen, C., Douma, W., Güven, O., and Rijken, T. (2017). *The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness*, *Study for the LIBE Committee*, Brussels: European Parliament, p.45: *http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf*.

84 Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*, p. 3. See also the European Council's dedicated webpage on 'Crisis and Terrorism' at *https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism_en*.

85 Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*, p. 4.

86 Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*, p. 7.

87 Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*, p. 8.

88 Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*, p. 9.

89 Council of the European Union (2005). *The European Union Counter-Terrorism Strategy*, p. 13.

90 Wensink *et al*. (2017). *The European Union's Policies on Counter-Terrorism*.

91 Council of the European Union (2005). *Strategy for Combating Radicalisation and Recruitment to Terrorism*. Brussels: Presidency, European Council: *http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014781%202005%20REV%201*.

92 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*. Brussels: Presidency, European Council: *http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf*, p. 3.

93 Council of the European Union (2005). *Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.3. Also See para 8 of 2008 strategy Council of the European Union (2008). Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, p. 4.

94 *Ibid*. Also See para 9 of 2008 strategy Council of the European Union (2008). Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, p. 4.

95 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p. 4.

96 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.6.

97 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.4.

98 *Ibid*.

99 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.5.

In terms of online radicalisation, this could include cooperation with internet companies, including social media platforms and other internet service providers (e.g. content hosting sites, online payment sites, messaging applications, etc.).

In terms of concrete actions to achieve the above aims and others detailed in the revised Strategy, mention is made of:

- …Ensuring that voices of mainstream opinion prevail over those of extremism;
- Enhancing government communications;
- Supporting messages countering terrorism;
- Countering online radicalisation and recruitment to terrorism;
- … Supporting further research into the trends and challenges of radicalisation and recruitment to terrorism;
- Align[ing] internal and external counter-radicalisation work. [100]

As regards strengthening non-extremist voices, the Strategy goes on to emphasise that in order for them to be heard"[t]hose voices must be communicated through an appropriate platform, such as mass and social media, which must be credible for the target audience".[101] It continues:

We must promote the development of tailor-made communication methods that challenge an extremist ideology which supports or is linked to terrorism either online or offline. It is key to communicate in a language appropriate to context and audience, using a range of credible and appropriate delivery channels, and to challenge radical or extremist communications at the platforms used most frequently by those who are most at risk to be radicalised. A one-size fits-all approach to communications will not work. At the same time, however, we must ensure consistency, clarity and continuity in our messaging at all levels.[102]

The use of the internet and social media is acknowledged as "critically important" in this respect, including in terms of its utilisation to promptly respond to "online rhetoric supporting terrorism and to reach those most vulnerable to radicalizing messages". The role of public-private partnership in achieving these aims is explicitly envisaged here.[103]

More specifically, paragraphs 30 – 32 of the 2014 Strategy compose a section headed 'Countering online radicalisation and recruitment to terrorism', which is worth quoting in its entirety:

The internet and social media can be used for the dissemination of propaganda material, fundraising, recruitment and communication with like-minded individuals, but also as a virtual training camp, as well as a means of exchanging skills and know-how. The internet is also a transnational entity transgressing various national jurisdictions.

Work to counter online radicalisation and recruitment to terrorism is wide-ranging. It covers activities aimed at disrupting terrorist use of the internet, but also initiatives to challenge the terrorist narrative. Some of it can be done at national or European level and some of it by people and organisations from within civil society, facilitated where necessary. Where content is illegal including material that is hosted in third countries, there must be processes in place to address the issue swiftly and effectively. This work will require effective dialogue with the private sector and in particular the internet industry, not only in Europe but also abroad. Efforts should also be made to use the internet and social media to promote counter narrative messages. All activities must be done in accordance with rule of law principles and in full respect of international human rights law.

We should continue to examine ways to actively prevent radicalisation and recruitment to terrorism by means of the internet and social media. We will address these issues as part of our Political Dialogues and we will offer technical support with the view of encouraging others, outside the EU, to do the same.[104]

Comparing the original and revised strategies, it is clear that the role of the internet, particularly social media, in radicalisation processes and responses to them was seen to be much greater in 2014 than in 2005.

It is also worth noting here that this Strategy echoes many of the core elements of the *EU Cyber Security Strategy* (discussed in Vol. 1 of this study), both in terms of the aspects of the issue that need to be addressed and also the type of approaches needed to address it. A good overall example of this is the way in which this Strategy, similar to the *EU Cyber Security Strategy*, recognises the transnational dimension of the internet and as a result the need for a joint effort at the local, regional, domestic, European, and international levels to respond to radicalisation and recruitment. Secondly, and again similar to the *Cyber Security Strategy*, the involvement of the private sector, on the basis that they bring different knowledge, tools, and resources often unavailable to governments, is foreseen.[105] The *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism* also promotes the development of public-private partnerships, noting that such relationships help to enhance trust and transparency. This need for trust was also identified in the *EU Cyber Security Strategy*. Finally, with respect to the portions of this strategy that resonate with the EU's *Cyber Security Strategy*, this Strategy also underlines the value of education sector involvement in this area, especially in raising awareness of terrorism-related issues and identifying and providing support to individuals at risk.

A number of other relevant EU Strategy Documents will now be highlighted.

3.1.3 EU Code of Conduct on Countering Illegal Hate Speech Online

In 2016, Facebook, Microsoft, Twitter, and YouTube committed to combatting the spread of illegal online hate speech in the EU through the voluntary Code of Conduct on Countering Illegal Hate Speech Online. The impetus for this closer relationship between IT companies and the EU was the terrorist attacks in Brussels in 2016, which resulted in a commitment by the EU Commission to "intensify work with IT companies, notably in the EU Internet Forum, to counter terrorist propaganda and to develop by June 2016 a code of conduct against hate speech online".[106] The code is based on a shared commitment to reduce the level of illegal hate speech online, stating:

While the effective application of provisions criminalising hate speech is dependent on a robust system of enforcement of criminal law sanctions against the individual perpetrators of hate speech, this work must be complemented with actions geared at ensuring that illegal hate speech online is expeditiously acted upon by online intermediaries and social media platforms, upon receipt of a valid notification, in an appropriate time-frame. .[107]

The Code aims to guide the activities of all IT companies that are signatories, as well as sharing best practices with other internet companies. To ensure this, the Code of Conduct sets out agreed commitments between the IT company signatories and the European Commission, including the IT companies putting in place "clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content"; "Rules or Community Guidelines clarifying that they prohibit the promotion of incitement to violence and hateful conduct"; dedicated teams to review valid removal notifications including, where necessary, transposing the Framework Decision 2008/913/JHA; measures such that valid notifications are reviewed in less than 24 hours and the content removed or disabled, if necessary; and "to educate and raise awareness with their users about the types of content not permitted under their rules and community guidelines". Also committed to by the IT companies is provision by them of information on the procedures for submitting notices, for purposes of "improving the speed and effectiveness of communication between the Member State authorities and the IT Companies", especially as regards notifications regarding disabling access to or removal of illegal hate speech. This information is to be channelled through national contact points designated by the IT companies and EU Member States respectively. This is described as enabling Member States, particularly their law enforcement agencies, to develop greater familiarity with available methods to recognise and notify the IT companies of illegal online hate speech.[108]

The need for CSO involvement is also addressed in the Code, with them described as having "a crucial role to play in the field of preventing the rise of hatred online, by developing counter-narratives promoting non-discrimination, tolerance and respect, including through awareness-raising activities".[109] The Code includes the following commitments in this regard:

- The IT companies to encourage the provision of notices and flagging of content that promotes incitement to violence and hateful conduct at scale by experts, particularly via partnerships with CSOs, by providing clear information on in-

100 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.5.

101 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.7.

102 *Ibid.*

103 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.8.

104 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p.9.

105 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*.

106 European Commission (2016). Code of Conduct on Countering Illegal Hate Speech Online, Strasbourg: European Commission, p.1: *https://edri.org/files/privatisedenf/euhatespeechcodeofconduct_20160531.pdf*.

107 European Union (2016). *Code of Conduct on Countering Illegal Hate Speech Online*, pp.'s 1-2.

108 European Union (2016). *Code of Conduct on Countering Illegal Hate Speech Online*, p.2.

109 European Union (2016). *Code of Conduct on Countering Illegal Hate Speech Online*, p.1; see also p.3.

dividual company Rules and Community Guidelines and rules on the reporting and notification processes. The IT Companies to endeavour to strengthen partnerships with CSOs by widening the geographical spread of such partnerships and, where appropriate, to provide support and training to enable CSO partners to fulfil the role of a "trusted reporter" or equivalent, with due respect to the need of maintaining their independence and credibility.

- The IT companies rely on support from Member States and the European Commission to ensure access to a representative network of CSO partners and "trusted reporters" in all Member States to help provide high quality notices. IT Companies to make information about "trusted reporters" available on their websites…
- The IT Companies and the European Commission, recognising the value of independent counter speech against hateful rhetoric and prejudice, aim to continue their work in identifying and promoting independent counter-narratives, new ideas and initiatives and supporting educational programmes that encourage critical thinking.
- The IT Companies to intensify their work with CSOs to deliver best practice training on countering hateful rhetoric and prejudice and increase the scale of their proactive outreach to CSOs to help them deliver effective counter speech campaigns. The European Commission, in cooperation with Member States, to contribute to this endeavour by taking steps to map CSOs' specific needs and demands in this respect.[110]

While not all the public commitments made in the Code have yet been fulfilled, progress has been achieved. The original four signatories of the Code were joined in 2018 by Instagram, Snapchat, and, most recently, Dailymotion.[111] Between signing the Code in 2016 and January 2018, the IT companies have removed around 70% of all illegal hate speech notified to them. This increased from 28% in 2016 and 59% up until May 2017. Furthermore, the IT companies were found to be increasingly fulfilling their commitment to take down illegal hate speech within one hour of a valid notification.[112]

110 European Union (2016). *Code of Conduct on Countering Illegal Hate Speech Online*, pp.'s 2-3.

111 See DG Justice and Consumers dedicated webpage 'Countering Illegal Hate Speech Online #NoPlace4Hate' for continuously updated news about the Code, including the newest signatories: *http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300*.

112 European Commission (2018). 'Countering Illegal Hate Speech Online: Commission Initiative Showing Continued Improvement', 19 January: *https://ec.europa.eu/ireland/news/countering-illegal-hate-speech-online-commission-initiative-showing-continued-improvement_en*.

3.1.4 Joint Action Plan on Counter-Terrorism for the Western Balkans

The *Joint Action Plan on Counter-Terrorism for the Western Balkans* was signed by the representatives of the WB6 and the EU at the Justice Home Affairs (JHA) Ministerial meeting in Tirana on 5 October 2018.[113] The plan:

Outlines a concrete level of ambition and focus common to all Western Balkans partners, as well as related EU support in the area of Counter-Terrorism, including Preventing and Countering of Violent Extremism. The five Counter-Terrorism objectives established in this plan should provide a common focus and lead to concrete deliverables in order to tackle the existing security challenges. This should include a systematic strengthening of regional cooperation.[114]

These objectives are:

Objective 1: A Robust Framework for Countering Terrorism and Preventing/Countering Violent Extremism: Institutional Set-up and Legal Alignment, Implementation and Enforcement Capacity.

Objective 2: Effective Prevention and Countering of Violent Extremism.

Objective 3: Effective Information Exchange and Operational Cooperation.

Objective 4: Build Capacity to Combat Money Laundering and Terrorism Financing.

Objective 5: Strengthen the Protection of Citizens and Infrastructure.[115]

Objective 2 specifically references online activities. It states that the each Western Balkans partner should seek to "[a]ddress terrorist content online, including by encouraging efforts to refer terrorist content to internet companies, and empowering civil society partners to develop effective alternative narratives online."[116] For their part the EU should, according to the Action Plan, "support Western Balkans partners' capacity to address terrorist content online, such as through Europol assistance, training and expertise, including the EU Internet Referral Unit of Europol's European Counter-Terrorism Centre (ECTC)". [117]

113 Council of the European Union (2018). *Joint Action Plan on Counter-Terrorism for the Western Balkans*. Brussels: General Secretariat of the Council: *http://www.statewatch.org/news/2018/sep/eu-council-joint-western-balkans-terror-action-plan-draft-11848-18.pdf*.

114 Council of the European Union (2018). *Joint Action Plan on Counter-Terrorism for the Western Balkans*, p.2.

115 Council of the European Union (2018). *Joint Action Plan on Counter-Terrorism for the Western Balkans*, pp.'s 4 – 14.

116 Council of the European Union (2018). *Joint Action Plan on Counter-Terrorism for the Western Balkans*, p.6.

While the Plan is not legally binding, it is intended that the objectives will be reached by December 2020.[118]

3.1.5 Other relevant EU documents

There are a variety of other EU documents and policies, besides those discussed above, that are relevant in the online radicalisation context, not all of which can be addressed here. Four additional documents are worth mentioning however; these are The European Agenda on Security (2015), the Council Conclusions on EU External Action on Counter-terrorism (2017), the final report of the High-Level Commission Expert Group on Radicalisation (HLCEG-R) (2018), and the Cyber Security Strategy of the European Union (2013).

The European Agenda on Security was adopted in April 2015. It resulted from the recognition that existing and emerging threats require an effective and coordinated response at European level. As a result, The European Agenda on Security is a shared agenda between the EU and Member States. It prioritises three areas, namely terrorism, organised crime, and cybercrime. In relation to extremist content, the Agenda states:

The EU must cut the support base of terrorism with a strong and determined counter-narrative. The Commission will ensure enforcement of relevant EU legislation in this area. It will assess any gaps in legislation and support the monitoring of online hate speech and other actions. It will also assist Member States in developing proactive investigation and prosecution practices on the ground. EU funding will increasingly be used to support specific training of public officials and encourage monitoring, reporting and recording of incidents of hate crime and hate speech.[119]

In the aftermath of the Charlie Hebdo attacks in France in January 2015, EU Member States affirmed the need for the EU to engage more with non-EU states in the area of security and counter-terrorism.[120] In July 2017, this resulted in publication of 'Council Conclusions on EU External Action on Counter-terrorism', which emphasised that greater consistency was required between internal and external actions in the counter-terrorism sphere and that DG Justice needed to be empowered to support this. Strengthening relationships with the Western Balkans was explicitly referenced in this document, including in relation to the foreign fighter phenomenon.[121] A lengthy paragraph on the role of the Internet in extremism and terrorism was also included; it stated:

The Council notes the growing challenges presented by online terrorist and extremist content and emphasises the need to effectively address online recruitment and radicalisation. The Council encourages Communication Service Providers, social media companies, broadcasters and other industry bodies to steadily increase their ongoing efforts to address these issues at a greater pace and scale, according to their terms of services. The Council welcomes industry's ongoing efforts in developing and sharing new technology and tools to improve their existing systems of automatic detection of, and removal of illegal content and to support positive alternative narratives in line with UNSCR 2354 and communication campaigns. The Council welcomes and supports the EU Internet Forum's efforts in bringing Member States and the industry together to address this urgent issue. The Council recognises the role of media in supporting alternative discourse to extremist content online and to combat hate speech, promote education on critical thinking and media literacy as important components in countering radicalisation to violent extremism.[122]

The final report of the High-Level Commission Expert Group on Radicalisation (HLCEG-R) was published in May 2018.[123] In their report, the Group

117 Council of the European Union (2018). *Joint Action Plan on Counter-Terrorism for the Western Balkans*, p.7.

118 Council of the European Union (2018). *Joint Action Plan on Counter-Terrorism for the Western Balkans*, p.2.

119 European Commission (2015). *European Union Agenda on Security*. Strasbourg: European Commission, p.15: *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf*.

120 See the official 'Counter-terrorism Strategy' information webpage at *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33275&from=EN*.

121 Council of the European Union (2017). 'Council Conclusions on EU External Action on Counter-terrorism'. Brussels, 19 June, p.'s 5, 6, 7 and 12: *https://www.consilium.europa.eu/media/23999/st10384en17-conclusions-on-eu-external-action-on-counter-terrorism.pdf*.

122 Council of the European Union (2017). 'Council Conclusions on EU External Action on Counter-terrorism', p.10.

123 High Level Commission Expert Group on Radicalisation (2018). *High Level Commission Expert Group on Radicalisation (HLCEG-R): Final Report*. Luxembourg: Publications Office of the European Union: *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180613_final-report-radicalisation.pdf*.

identified a number of priority areas where further action at EU level could offer significant benefit, including in regard to communication and countering online propaganda. In the Report's introduction the Group states:

Irrespective of the kind of radicalisation or country-specific circumstances, Member States are confronted with similar concerns such as the use of the internet and social media by terrorist groups or violent extremist organisations for propaganda and recruitment purposes…Despite significant setbacks on the ground, Daesh continues to devote considerable effort to its media operation and early this year saw resurgence in media production. The internet tended to feature prominently in almost every attack that happened in 2017, whether it was in using online instructions to prepare for the attack or glorifying in its aftermath, and it is clear that terrorist groups continue to use the internet to groom and recruit. In addition to Daesh propaganda, other terrorist groups similarly exploit the internet for terrorist gain. Al Qaeda, Boko Haram and a worrying rise of violent right-wing extremists are all prolific users of the internet, challenging the cohesion of Europe's societies.[124]

Interestingly, while the Group acknowledges the work done in this area, it also makes a number of recommendations, two of which are particularly worth noting. First, "the Group calls for action as regards traditional media and satellite television misused to amplify the terrorist and extremist divisive narrative, and to promote responsible media reporting".[125] Today the role of traditional or mass media is often overlooked, in favour of a focus on the internet, particularly social media. The Group's recommendation that EU MS's and the Commission "examine whether existing tools (including legislation) are sufficient to effectively prevent the spread of violent extremist propaganda via traditional media including satellite TV as well as initiating a structured dialogue with media companies on illegal content"[126] is therefore a worthwhile corrective. Also because the press and satellite television broadcasters are increasingly reliant on the internet for various of their functions. Second, the Group makes an explicit link between terrorism and extremism, on the one hand, and fake news, on the other, and recommends further analysis on "how disinformation and fake news influence terrorist and extremist groups' ability to impact audiences, supplementing ongoing work in this area as set out in the Communication on disinformation".[127] The latter includes the observation that disinformation "often supports radical and extremist ideas and activities".[128]

The role of the EU's Cyber Security Strategy should also be acknowledged in this volume, albeit it is discussed in more detail in Vol. 1. While the Cyber Security Strategy does not specifically refer to online radicalisation and extremism or information operations, it does refer to terrorism, acknowledging that cyber threats can have "different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes". Furthermore, the strategy recognises challenges in the area of cyber security that are echoed in relation to information operations, including online radicalisation and extremism. For example, it highlights "the borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation",[129] a feature often exploited by producers and distributors of extremist content online. Furthermore, in its recognition that the internet is not controlled by a single entity, it explicitly notes the need for more engagement and better partnerships, outlining a commitment to:

Engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries to improve access to information and to an open Internet, to prevent and counter cyber threats, including accidental events, cybercrime and cyber terrorism, and to develop donor coordination for steering capacity-building efforts.[130]

Given these elements, the Cyber Security Strategy is structured in a manner that would support the inclusion of information operations and attacks within the context of cyber security. Furthermore, it explicitly identifies the need for cyber security to protect fundamental rights, freedom of expression, personal data, and privacy, which is pertinent with respect to online extremism and terrorism, given the competing forces of free speech and anti-extremism.

Despite security and terrorism being the primary responsibility of individual EU Member States, these documents serve to illustrate the level of awareness within the EU that a shared approach is required in this area, both internally and externally. This could be a model for the WB6.

3.2 EU Legislation

3.2.1 EU Counter Terrorism Directive

EU Directive 2017/541 on Combatting Terrorism was signed in March 2017, replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.[131] Similar to the Framework Decision, the Directive:

Establishes minimum rules concerning the definition of criminal offences and sanctions in the area of terrorist offences, offences related to a terrorist group and offences related to terrorist activities, as well as measures of protection of, and support and assistance to, victims of terrorism.[132]

The Directive sets out a number of specific terrorist related offences. These include public provocation to commit a terrorist offence (Article 5), recruitment for terrorism (Article 6), providing training for terrorism (Article 7), receiving training for terrorism (Article 8), organising or otherwise facilitating travelling for the purpose of terrorism (Article 10), and terrorist financing (Article 11). All of these can have online components. Article 5 regarding public provocation to commit a terrorist offence, specifically refers to online activities:

Member States shall take the necessary measures to ensure that the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Article 3(1),[133] where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed, is punishable as a criminal offence when committed intentionally.[134]

In addition, Article 21 of the Directive relates to measures against public provocation, including via the internet, stating that:

1. Member States shall take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence, as referred to in Article 5, that is hosted in their territory. They shall also endeavour to obtain the removal of such content hosted outside their territory.
2. Member States may, when removal of the content referred to in paragraph 1 at its source is not feasible, take measures to block access to such content towards the internet users within their territory.
3. Measures of removal and blocking must be set following transparent procedures and provide

124 High Level Commission Expert Group on Radicalisation (2018). *HLCEG-R: Final Report*, p.3.

125 High Level Commission Expert Group on Radicalisation (2018). *HLCEG-R: Final Report*, p.7.

126 High Level Commission Expert Group on Radicalisation (2018). *HLCEG-R: Final Report*, p.8.

127 High Level Commission Expert Group on Radicalisation (2018). *HLCEG-R: Final Report*, p.7; see also p.8.

128 European Commission (2018). 'Tackling Online Disinformation: A European Approach', Brussels, 26 April, p.1: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&rid=2*.

129 European Commission (2013). *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: High Representative of the European Union for Foreign Affairs and Security Policy, p. 3: *http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf*.

130 European Commission (2013). *Cyber Security Strategy of the European Union*, p.16.

131 Council Directive 2017/541/EU on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN*.

132 Council Directive 2017/541/EU on Combating Terrorism, p. 12.

133 Article 3(1) of Council Directive 2017/541/EU on Combating Terrorism states on p.13 that "1. Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2: (a) attacks upon a person's life which may cause death; (b) attacks upon the physical integrity of a person; (c) kidnapping or hostage-taking; (d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss; (e) seizure of aircraft, ships or other means of public or goods transport; (f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons; (g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life; (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life; (i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council (1) in cases where Article 9(3) or point (b) or (c) of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies; (j) threatening to commit any of the acts listed in points (a) to (i). 2. The aims referred to in paragraph 1 are: (a) seriously intimidating a population; (b) unduly compelling a government or an international organisation to perform or abstain from performing any act; (c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation."

134 Council Directive 2017/541/EU on Combating Terrorism, p.14.

adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress.[135]

Interestingly, the Directive also refers to attacks on information systems, particularly referencing attacks:

[C]ausing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss.[136]

The importance of this EU Directive is evident as it legislates for shared responses to terrorism by Member States. Despite this, and unlike the NIS Directive (see Vol.1), it was not heavily referenced in interviews as a fundamental underpinning of legislative frameworks within WB6. This is not to say that it did not influence responses to online radicalisation within the WB6, but just that it was not explicitly referred to by interviewees as having done so.

3.2.2 Forthcoming EU legislation

On 12 September 2018, on the occasion of his State of the Union Address, EU President Jean-Claude Juncker announced new rules "to get terrorist content off the web".[137] The purpose of these new rules is, at least partially, to ensure that terrorist content is removed more swiftly than heretofore.[138] The key features of the new rules are:

- **The one-hour rule:** Terrorist content is most harmful in the first hours after it appears online because of the speed at which it spreads. This is why the Commission is proposing a legally binding one-hour deadline for content to be removed following a removal order from national competent authorities;
- **A clear definition of terrorist content** as material that incites or advocates committing terrorist offences, promotes the activities of a terrorist group or provides instruction in techniques for committing terrorist offences;
- **A duty of care obligation** for all platforms to ensure they are not misused for the dissemination of terrorist content online. Depending on the risk of terrorist content being disseminated via their platforms, service providers will also be required to take proactive measures – such as the use of new tools – to better protect their platforms and their users from terrorist abuse;
- **Increased cooperation:** The proposal sets up a framework for strengthened co-operation between hosting service providers, Member States and Europol. Service providers and Member States will be required to designate points of contact reachable 24/7 to facilitate the follow up to removal orders and referrals;
- **Strong safeguards:** Content providers will be able to rely on effective complaint mechanisms that all service providers will have to put in place. Where content has been removed unjustifiably, the service provider will be required to reinstate it as soon as possible. Effective judicial remedies will also be provided by national authorities and platforms and content providers will have the right to challenge a removal order. For platforms making use of automated detection tools, human oversight and verification should be in place to prevent erroneous removals;
- **Increased transparency and accountability:** Transparency and oversight will be guaranteed with annual transparency reports required from service providers and Member States on how they tackle terrorist content as well as regular reporting on proactive measures taken;
- **Strong and deterrent financial penalties:** Member States will have to put in place effective, proportionate and dissuasive penalties for not complying with orders to remove online terrorist content. In the event of systematic failures to remove such content following removal orders, a service provider could face financial penalties of up to 4% of its global turnover for the last business year.[139]

EU President Juncker also included in his State of the Union Address a proposal to "extend the tasks of the newly established European Public Prosecutor's Office to include the fight against terrorist offences", noting that the EU cannot be unwitting accomplice due to an inability to cooperate.[140] The EU Commission also produced a State of the Union Factsheet on Building strong cybersecurity in Europe, setting out a number of other commitments in this area. The Factsheet noted that Commission is complement existing efforts with

the creation of a Network of Competence Centres and a European Cybersecurity Industrial, Technology and Research Competence Centre to develop and roll out the tools and technology needed to keep up with an ever-changing threat. The European Centre will be in charge of coordinating the funds foreseen for cybersecurity in the next long-term EU budget together with the Member States in the most targeted way. This will help to create new European cyber capabilities.[141]

Not only would these be beneficial in relation to cyber security, they also have the potential to have a positive impact in relation to (dis-)information operations, including not just online radicalisation and extremism, but also so-called 'fake news' and related issues.

3.3 EU agencies and networks

The EU has established a number of organisations to help provide systematic support on extremism, terrorism, and the Internet, and their intersections, to Member States. A number of these are discussed below. This is not an exhaustive list, but those highlighted represent the key organisations with an online focus.

3.3.1 European Union Internet Forum (EUIF)[142]

The European Union Internet Forum (EUIF) was established in December 2015 to bring together EU Interior Ministers, high-level representatives of major internet companies, Europol, the EU Counter Terrorism Co-ordinator and the European Parliament to counter both online hate speech and terrorist content,[143] one of the key commitments made in the *European Agenda on Security*. The aim of the Forum is to reach a jointly agreed voluntary approach to detecting and addressing harmful online content, through a public-private partnership approach. Key areas of discussion have included "how to protect the public from the spread of terrorist material and terrorist exploitation of communication channels to facilitate and direct their activities" and "how to make better use of the Internet to challenge terrorist narratives and online hate speech". [144] This has resulted in:

[A] referral mechanism with the participation of Europol to remove internet content; the creation of a prototype database of hashes developed by the internet industry to create a shared database to help identify potential terrorist content on social media and prevent its reappearance on other platforms; and the establishment of a Civil Society Empowerment Programme.[145]

This approach puts into practice a longstanding recognition on the part of the EU that the private sector, in this case social media and other internet companies, have a significant role to play in the fight against online radicalisation and incitement to violence.

3.3.2 EU Internet Referral Unit (EU IRU)[146]

The EU Internet Referral Unit (EU IRU) was also established in 2015 and is a component of Europol's European Counter Terrorism Centre (ECTC). The IRU was established based on recognition of the increased amounts of terrorist content, particularly violent jihadi content, available online, and targeting multiple language audiences, irrespective of borders. The unit's core tasks are:

- Supporting the competent EU authorities by providing strategic and operational analysis;
- Flagging terrorist and violent extremist online content and sharing it with relevant partners;

135 Council Directive 2017/541/EU on Combating Terrorism, p.18.

136 Council Directive 2017/541/EU on Combating Terrorism, p.13.

137 Jean-Claude Juncker (2018). 'State of the Union 2018: The Hour of European Sovereignty', Brussels, 12 September, p.7: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en_0.pdf.

138 *Ibid*.

139 European Commission (2018). 'State of the Union 2018: Commission Proposes New Rules to Get Terrorist Content Off the Web, Brussels, 12 September: *http://europa.eu/rapid/press-release_IP-18-5561_en.htm*.

140 Jean-Claude Juncker (2018). 'State of the Union 2018, p.7.

141 European Commission (2018). 'State of the Union Factsheet on Building Strong Cybersecurity in Europe', Brussels, 12 September: *https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_en.pdf*.

142 By way of full disclosure, Prof. Maura Conway is Coordinator of the EU-funded VOX-Pol network, which is a regular contributor to the Forum.

143 European Commission (2015). ' EU Internet Forum: Bringing Together Governments, Europol and Technology Companies to Counter Terrorist Content and Hate Speech Online', *Press Release*, Brussels, 3 December: *http://europa.eu/rapid/press-release_IP-15-6243_en.htm*.

144 *Ibid*.

145 European Commission (2017). 'EU Internet Forum: Progress on Removal of Terrorist Content Online', San Francisco, 10 March: *http://europa.eu/rapid/press-release_IP-17-544_en.htm*.

146 By way of full disclosure, Prof. Conway is a member of the Steering Committee of the Europol Counter-terrorism Centre's Advisory Network.

- Detecting and requesting removal of internet content used by smuggling networks to attract migrants and refugees;
- Swiftly carrying out and supporting the referral process, in close cooperation with the [internet] industry.[147]

The IRU is made-up of experts in religiously-inspired terrorism, translation, information and communications technology, and counter terrorism law enforcement professionals, which results in a multi-disciplinary team.[148] According to its webpage, the Unit had by December 2017 "assessed in total 42,066 pieces of content, which triggered 40,714 decisions for referral across over 80 platforms in more than 10 languages. On average, the content flagged for referrals has been removed in 86% of the cases".[149]

3.3.3 Radicalisation Awareness Network (RAN)

The EU's Radicalisation Awareness Network (RAN) was established in 2011; it "facilitates the exchange of best practices and expertise, consolidates knowledge and identifies and develops best practices, concrete guidance and tailor made support services".[150] It was established under the EU Internal Security Strategy in Action, connecting people from keys groups, such as "researchers, social workers, religious leaders, youth leaders, policemen and others working on the ground in vulnerable communities".[151] Since its establishment, the RAN has brought together over 2,000 professionals from all Member States, through the RAN Centre of Excellence (CoE).

The CoE guides the activity of the RAN's Working Groups. These groups aim for their members to "meet peers from around Europe, build up new, long-lasting relationships, draw inspiration from one another and peer review best practices". There are Working Groups devoted to Education (RAN EDU), exiting extremist and terrorist organisation (RAN EXIT), Youth, Families and Communities (RAN YF&C), Local Authorities (RAN LOCAL), Prison and Probation (RAN P&P), Police and Law Enforcement (RAN POL), Remembrance of Victims of Terrorism (RAN RVT), Health and Social Care (RAN H&SC), and Communication and Narratives (RAN C&N). The latter is the most relevant for those working in the area of online extremism and radicalisation. It is tasked with "formulating and delivering on- and offline communication tools challenging extremist propaganda and/or providing alternatives to extremist ideas".[152] It aims to do this by "gather[ing] insights on both online and offline communication that 1) offers alternatives to or 2) counters extremist propaganda and/or challenges extremist ideas". The Working Group is focused not just on the content of these narratives, but also their target audiences, and utilising credible counter messengers (e.g. civil society, victims, former extremists, and youth) and a multiplicity of dissemination pathways (e.g. face-to-face interventions, testimonials in class rooms, blogs, chatrooms, websites, and social media) to mitigate their effects.[153]

3.4 Additional programmes and activities

As referenced in, amongst other documents, the 'Council Conclusions on EU External Action on Counter-terrorism', the EU has identified the need to look beyond Member States and to work with other economies in the fight against terrorism, including online. The EU's work in this regard segues very well with the efforts of a number of other organisations active in this area. The work of the OSCE, Council of Europe, Global Internet Forum to Counter Terrorism, United Nations Counter Terrorism Committee (UNCTC), and NATO is profiled below. Again, this is not an exhaustive list; the focus is on organisations active in the WB6 or whose activities may have relevance for the WB6.

3.4.1 Council of Europe

As mentioned in Vol. 1, the Council of Europe's Budapest Convention on Cybercrime (2001) is the only legally binding multilateral instrument that specifically addresses cybercrime. It does this by, *inter alia*, providing a common legal framework for international co-operation against cybercrime between States parties to the Convention. Furthermore, its additional Protocol concerns the criminalisation of acts of a racist and xenophobic nature[154] committed through computer systems. Article 3 of this protocol relating to dissemination of racist and xenophobic material through computer systems, states:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.
3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.[155]

Other CoE protocols are also very relevant in this area. For example, the *Council of Europe Convention on the Prevention of Terrorism* (CETS No. 196), which came into force in June 2007:

Aims to support and strengthen the fight against terrorism while reaffirming that all measures taken to prevent or suppress terrorist offences have to respect the rule of law and democratic values, human rights and fundamental freedoms…The Convention is aimed at improving national counter-terrorism policies and strategies at the domestic level while also facilitating effective international co-operation and mutual legal assistance in criminal matters.[156]

The Convention calls for the establishment of appropriate national terrorism prevention policies and establishes several acts as criminal offences, including public provocation to commit a terrorist offence (Article 5), recruitment for terrorism (Article 6), and training for terrorism (Article 7). While not explicitly referred to in the Articles, all of these may clearly have online components, particularly public provocation, which is described in Article 5 as "the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence". Though clearly "solicit[ing] another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group" (Article 6) and "provid[ing] instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence" (Article 7) could also be carried wholly or partially via the Net.

This Convention was further enhanced in 2015 with the adoption of an Additional Protocol (CETS No. 2017), which "addresses the main substantive criminal law elements of the United Nations Security Council resolution 2178 (2014) aimed at enhancing international co-operation to prevent and prosecute persons travelling for the purposes of terrorism".[157] The Protocol added new offences, such as "participating in an association or group for the purposes of terrorism (Article 2), receiving training for terrorism (Article 3), travelling abroad for the purpose of terrorism (Article 4), funding travelling abroad for the purpose of terrorism (Article 5), and organising or otherwise facilitating travelling abroad for the purpose of terrorism (Article 6)".[158] Again, all of these activities may be carried out either wholly or partially online.

The CoE also has a Committee on Counter Terrorism (CDCT), previously the Committee of Experts on Terrorism (CODEXTER). It is an intergovernmental body coordinating the CoE's action against terrorism. The CDCT is "tasked with developing appropriate and practical soft law instruments such as

147 See the EU IRU's dedicated webpage at *https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru*.

148 *Ibid*.

149 *Ibid*.

150 European Commission (2015). 'EU Internet Forum: Bringing together Governments, Europol and Technology Companies.

151 See the RAN's dedicated webpage at *https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/radicalisation_en*.

152 See European Commission on The Radicalisation Awareness Network – a practitioners' network, p. 1, *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/docs/ran_leaflet_en.pdf*

153 RAN C&N (2015). 'RAN C&N: Ex-post Paper'. Berlin, 10 – 11 Dec., p.1: *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-c-and-n/docs/ran_c-n_counter_and_alternative_narratives_berlin_10-11122015_en.pdf*.

154 According to Article 2 of the Additional Protocol, "*Racist and xenophobic material* means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors". See Council of Europe (2003).
'Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems', Strasbourg, 28 January: *https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f*.

155 Council of Europe (2003). 'Additional Protocol to the Convention on Cybercrime, Article 3.

156 See Council of Europe Webpage 'The 2005 Warsaw Convention and its Additional Protocol' at *https://www.coe.int/en/web/counter-terrorism/cdct/warsaw-convention-and-additional-protocol*.

157 *Ibid*.

158 *Ibid*.

recommendations and guidelines for member States to consider and apply in the fight against terrorist activity".[159] Its key priorities for 2018 and 2019 are:

Developing a Council of Europe Counter-Terrorism Strategy 2018-2022;

Examining the feasibility of agreeing to a pan-European legal definition of "terrorism" for the 2005 Warsaw Convention;

Addressing the phenomena of foreign terrorist fighters and returnees;

The use and abuse of the internet by terrorists;

The roles of women and children in terrorism;

Links between terrorism and organised crime (to be addressed in cooperation with the European Committee on Crime Problems (CDPC).[160]

In July 2018, the COE achieved the first priority, by adopting a new counter terrorism strategy for 2018-2022. Two of the three strands, prevention, prosecution and protection, contain specific reference to the internet. These include:

Prevention

1.2 Preventing and countering terrorist public provocation, propaganda, radicalisation, recruitment and training on the internet

Activity: compilation of best practices on how to prevent and counter terrorist public provocation, propaganda, radicalisation, recruitment and training on the internet, while respecting human rights and fundamental freedoms, the rule of law and democracy.

Prosecution

2.2 Gathering of e-evidence in terrorism related cases

Activity: developing guidelines, for the gathering of e-evidence on the internet for the purpose of prosecution of suspected terrorists.

3.4.2 OSCE

One of the OSCE's first pronouncements on fighting terrorism was its 2002 *Charter on Preventing and Countering Terrorism*, which included a commitment "to combat hate speech and to take the necessary measures to prevent the abuse of the media and information technology for terrorist purposes."[161] This was followed-up by two OSCE Ministerial Council decisions on 'Combating the Use of the Internet for Terrorist Purposes', published in 2004 and 2006 respectively. A relevant aspect of the 2004 Decision is that it 'recalls' the June 2004 OSCE Meeting on the Relationship Between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes in this context.[162] By 2006, the OSCE was describing itself as "gravely concerned with the growing use of the Internet for terrorist purposes".[163] As a result, decision No. 7/06, Countering the Use of the Internet for Terrorists Purposes notes that:

Taking into account different national approaches to defining "illegal" and "objectionable" content and different methods of dealing with illegal and objectionable content in cyberspace, such as the possible use of intelligence collected from Internet traffic and content to closing websites of terrorist organizations and their supporters [and] Concerned with continued hacker attacks, which though not terrorism related, still demonstrate existing expertise in the field and thus providing a possibility of terrorist cyber attacks against computer systems, affecting the work of critical infrastructures, financial institutions or other vital networks, the [OSCE]

1. Decides to intensify action by the OSCE and its participating States, notably by enhancing international co-operation on countering the use of the Internet for terrorist purposes;[164]

6. Invites participating States to increase their monitoring of websites of terrorist/violent extremist organizations and their supporters and to invigorate their exchange of information in the OSCE and other relevant fora on the use of the Internet for terrorist purposes and measures taken to counter it, in line with national legislation, while ensuring respect for international human rights obligations and standards, including those concerning the rights to privacy and freedom of opinion and expression, and the rule of law. Duplication of efforts with ongoing activities in other international fora should be avoided;[165]

7. Recommends participating States to explore the possibility of more active engagement of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes.[166]

In 2012, the OSCE produced its *Consolidated Framework for the Fight against Terrorism*.[167] The document built on the OSCE's previous work on countering terrorism, with the objective to enhance "the profile and added value of the OSCE's contribution to the global efforts to eradicate terrorism and at facilitating communication and strengthening co-operation with key partners and organizations".[168] The Framework identifies eight strategic focus areas for OSCE counter-terrorism activities, one of which is "[c]ountering use of the Internet for terrorist purposes".[169] A related focus area is "[p]romoting dialogue and co-operation on counter-terrorism issues, in particular, through public-private partnerships between State authorities and the private sector (business community, industry), as well as civil society and the media".[170]

In September 2017, the Action against Terrorism Unit of the OSCE's Transnational Threats Department also launched an online learning course designed to raise awareness, knowledge and understanding on how terrorists use the internet. The course is titled *Countering the Use of the Internet for Terrorist Purposes* and aims to educate decision makers, government officials, academia, teachers and students in police academies and other similar educational institutions on "how the internet is a key strategic device and tactical facilitator in the hands of terrorists, who go online to identify, recruit and train new members, collect and transfer funds, organize attacks and incite violence".[171]

OSCE also work in the area of countering violent extremism, with much of their work done in the WB6.

3.4.3 Global Internet Forum to Counter Terrorism (GIF-CT)

Somewhat of a turning point was reached in 2017 as regards developments in tackling violent extremism and terrorism online, with major tech companies displaying an increased willingness to take down certain content from their platforms due, at least in part, to reputation and economic damage arising from attention to this content and the European Union and some of its Member State governments exhibiting decreased willingness to proceed at the tech companies' pace, and instead start implementing legislation to restrict the dissemination of extremist content online.

The Global Internet Forum to Counter Terrorism (GIF-CT) was established in 2017 by Facebook, Microsoft, Twitter, and YouTube as a result of their cooperation under the auspices of the EUIF. The objective of the GIF-CT is "to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using our platforms".[172] Practically, the GIF-CT is committed to achieving this through employing and leveraging appropriate technology; sharing knowledge, information and best practices; and conducting and funding research. Similar to the EU, UN, and other organisations referenced above, the GIF-CT recognises the need for collaboration with a wide range of stakeholders to achieve their objectives. They presently work closely with the UN Counter Terrorism Executive Directorate (UN CTED) and its Tech Against Terrorism initiative in this regard. The GIF-CT also recognises the need "to preserve and respect the fundamental human rights that terrorism seeks to undermine, including free expression, the role of journalism, and user privacy".[173] To do this, they work with human rights experts and other civil society stakeholders. The four companies are also looking to "cutting-edge technological solutions such as photo and video matching and text-based machine learning classification techniques" to help them deliver results, with much of this technology already in use.[174]

3.4.4 United Nations Security Council Counter-Terrorism Committee (UNCTC)

The United Nations Global Counter-Terrorism Strategy seeks to explore ways and means to "coordi-

159 See Council of Europe webpage 'Council of Europe Counter-Terrorism Committee (CDCT)' at *https://www.coe.int/en/web/counter-terrorism/cdct*.

160 *Ibid*.

161 OSCE Ministerial Council (2002). *Charter on Preventing and Countering Terrorism*. Vienna: OSCE, p.3: *https://www.osce.org/odihr/16609?download=true*.

162 OSCE Ministerial Council (2004). 'Decision No. 3/04 Combating the Use of the Internet for Terrorist Purposes', Sofia, 7 Dec., p.1: *https://www.osce.org/mc/42647?download=true*.

163 OSCE Ministerial Council (2006). 'Decision No. 7/06 Countering the Use of the Internet for Terrorist Purposes', Brussels, 5 Dec., p.1: *https://ccdcoe.org/sites/default/files/documents/OSCE-061205-CounteringUseofInternet.pdf*.

164 OSCE (2006). 'Decision No. 7/06 Countering the Use of the Internet for Terrorist Purposes', p.2.

165 OSCE (2006). 'Decision No. 7/06 Countering the Use of the Internet for Terrorist Purposes', p.3.

166 *Ibid*.

167 OSCE Permanent Council (2012). *Consolidated Framework for the Fight against Terrorism*. Vienna: OSCE: *https://www.osce.org/pc/98008?download=true*.

168 OSCE (2012). *Consolidated Framework for the Fight against Terrorism*, p.1.

169 OSCE (2012). *Consolidated Framework for the Fight against Terrorism*, p.5.

170 OSCE (2012). *Consolidated Framework for the Fight against Terrorism*, p.5.

171 OSCE (2017). 'OSCE Launches E-learning Course to Raise Awareness on How the Internet is Used for Terrorist Purposes', *Press Release*, 22 Sept.: *https://www.osce.org/secretariat/344926*.

172 See official GIF-CT website at https://gifct.org/.

173 *Ibid*.

174 *Ibid*.

nate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet" and to "use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard"[175], given that the UN Counter-Terrorism Committee (UNCTC) (S/2006/737 of 15 September 2006) noted that several States reported "they are studying the application of the prohibition on incitement in their national legislation to the Internet".[176]

The aim of the UNCTC is to help improve UN Member States to prevent terrorist acts. The impetus for its establishment was the September 11 attacks in the US in 2001. The United Nations Counterterrorism Executive Directorate (UNCTED) was established to assist the UNCTC. UNCTED "carries out the policy decisions of the Committee, conducts expert assessments of each Member State and facilitates counter-terrorism technical assistance to countries".[177] This includes responsibility for addressing "the use of ICT in terrorist activities, in consultation with Member States, international, regional, and sub-regional organizations, the private sector, and civil society, and to advise the Committee on further approaches".[178]

The related work of CTED focuses on four pillars: (i) mainstreaming ICT in its assessment of Member States' implementation of resolutions 1373 (2001), 1624 (2005), and 2178 (2014); (ii) the promotion of industry self-regulation; (iii) strengthening mutual legal assistance regarding digital content; and (iv) promoting counter-messaging techniques, including online. [179]

UNCTED organises events on countering terrorism through the use of ICT. It is also engaged directly with two specific initiatives. One is conducted together with the Swiss Foundation ICT4Peace. This programme works with the private sector and civil society to increase their "understanding of industry responses to the use of new technology for terrorist purposes and identify good practices". [180] The second initiative is carried out in association with the International Association of Prosecutors (IAP) and the United Nations Office on Drugs and Crime (UNODC). It "focuses on strengthening international cooperation among national prosecutors engaged in counter-terrorism issues, notably by enhancing their capacity to obtain evidence in a timely manner". [181]

Another example of the UN's work in this area is Tech Against Terrorism a

UN-mandated initiative that helps tech companies prevent their platforms from being exploited by terrorists, while also respecting human rights. Tech Against Terrorism works with the global tech sector to share best practice (policy, guidelines, learning materials, practical workshops, and tools) within the tech industry and with governments. The vast majority of our work is based on our consultations with tech companies across the world.[182]

Since 2017, it has launched the Knowledge Sharing Platform, which is a collection of tools that start-ups and small tech companies can use to better protect themselves from the terrorist exploitation of their services. Tech Against Terrorism collaborates with the GIF-CT, as discussed above.

Going forward, UNCTED aims to continue:

To mainstream ICT into its current and future activities, notably those relating to terrorism financing, bringing terrorists to justice, regional and international cooperation, and the protection of critical infrastructures, within the framework of its efforts to assist the Committee to monitor the implementation of the relevant Council resolutions.[183]

3.4.5 NATO

NATO hosts a number of "Centres of Excellence", two of which relate to countering terrorist narratives. The first was established in 2014, and is called the Strategic Communications Centre of Excellence and is based in Riga, Latvia. In the last number of years, the network has increasingly looked at the emerging risks of social media, which has included exploring issues such as Violent Extremism as an emerging threat for NATO nations, the weaponising of social media, and data exploitation by malicious actors.[184] The second relevant NATO Centre of Excellence is focused on Defence Against Terrorism and is based in Ankara, Turkey. Its aim is "to prevent non-conventional attacks, such as suicide attacks with improvised explosive devices (IEDs), and mitigate other challenges, such as attacks on critical infrastructure".[185] To do this NATO is developing new technologies and capabilities to help protect both military and civilians against terrorist attacks.

3.5 Funding

As mentioned above, much of the funding for dedicated activities comes from the European Commission. However, other funding does exist. One example is the EU's Internal Security Fund (ISF). Between 2014 and 2020 it is expected that the ISF-Police national programmes will fund projects relating to radicalisation to the value of €314 million.[186] The European Commission also funds research in this area, most recently via European Union Framework Programme 7 (FP7) and its follow-up, Horizon 2020. Examples of currently underway funded projects relating specifically to online content search, analysis, and related are Pericles,[187] TAKEDOWN,[188] Tensor,[189] and VOX-Pol.[190],

Overall, this section serves to illustrate the wide array of actions and activities conducted by the EU and others in the area of online radicalisation and extremism. It is evident that while some activities are directed specifically at online content, activities and messaging, others are much broader in scope, dealing with issues like social inclusion, awareness raising, etc. However, it is worth noting that few, if any, include an explicit recognition for a greater complementarity of approach between online radicalisation and extremist content and cyber security. Nonetheless, they serve to illustrate not only a shared recognition for the need for broader engagement in responding to these issues but they also act as concrete examples for successful public-private partnerships, activities in the education sector, and interdisciplinary responses, that are much needed in this area. The next section will examine how such activities and actions have influenced developments within the WB6.

175 United Nations General Assembly (2006). *The United Nations Global Counter-Terrorism Strategy*. New York: United Nationsp.6: *http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288*.

176 OSCE (2006). 'Decision no. 7/06 Countering the Use of the Internet for Terrorist Purposes', p.1.

177 See the official UNCTC website at *https://www.un.org/sc/ctc/*.

178 See UNCTC webpage on 'Information and Communication Technology' at *https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/*.

179 *Ibid*.

180 *Ibid*.

181 *Ibid*.

182 See the Tech Against Terrorism website at *https://www.techagainstterrorism.org/about/*.

183 *Ibid*.

184 See official NATO StratCom Centre of Excellence webpage at *https://www.stratcomcoe.org/program-work*.

185 See official NATO webpage on 'Defence Against Terrorism Programme of Work (DAT POW)' at *https://www.nato.int/cps/en/natohq/topics_50313.htm*.

186 ANP (2016). 'European Commission: Stronger Action at EU Level to Better Tackle Violent Radicalisation', *ANP*, 14 June: *https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vk4xg4q3rtx9?ctx=vga3buzdwirl&v=1&tab=1&start_tab0=280*.

187 For more information, see *http://project-pericles.eu/*.

188 For more information, see *https://www.takedownproject.eu/*.

189 For more information, see *https://tensor-project.eu/*.

190 For more information, see *http://www.voxpol.eu*.

4. ONLINE RADICALIZATION AND EXTREMISM IN THE REGION

This section details progress made and continuing challenges within the WB6 in respect to online radicalisation and extremism.

4.1 Legislation, strategies, and policies

Countries globally have in the past number of years devised national-level strategies for countering radicalisation and/or violent extremism (CVE). That said, use of the internet for terrorism purposes is mentioned in BiH's Strategy for Preventing and Combating Terrorism 2015 - 2020 albeit online radicalisation is not specifically referred to.[191] Similarly, Serbia's National Strategy for the Prevention and Countering of Terrorism 2017-2021 mentions radicalisation on the internet, but does not expand upon it.[192] Some WB6 economies with dedicated CVE strategies discuss the meaning of extremism and/or radicalisation within their strategies and address online radicalisation.

The Former Yugoslav Republic of Macedonia's *National Strategy for Countering Violent Extremism* identifies "terrorist radicalisation" as a "dynamic process whereby an individual comes to accept terrorist violence as a possible, perhaps even legitimate, course of action."[193] Both Albania and Montenegro's National Strategy employ the terminology of "radicalisation to violence," described as "a decision to forgo political processes or nonviolent methods of fostering change in favour of adopting violent methods to bring about change,"[194] which is based upon the meanings defined by the UN Working Group on Radicalization and Extremism that Lead to Terrorism and the Global Fund for Community

191 Government of Bosnia Herzegovina, 2015. *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism, 2015-2020*. Sarajevo: *http://msb.gov.ba/PDF/STRATEGIJA_ZA_BORBU_PROTIV_TERORIZMA_ENG.pdf*.

192 Government of Serbia (2017). *National Strategy for the Prevention and Countering of Terrorism, 2017-2021*: *https://rm.coe.int/serbian-national-strategy-for-the-prevention-and-countering-of-terrori/168088ae0b*.

193 Government of the [The Former Yugoslav Republic of Macedonia]. 2018. *National Committee for Countering Violent Extremism and Countering Terrorism*, 2018 – 2022, Skopje: *http://vlada.mk/sites/default/files/dokumenti/ct_national_strategy_eng_translation_sbu.pdf*, p.11.

194 Republic of Albania (n.d.). *Albanian National Strategy Countering Violent Extremism* (Unofficial Translation), Tirana, p.4: *https://www.rcc.int/p-cve/download/docs/Albanian%20National%20Strategy%20on%20Countering%20Violent%20Extremism.pdf/eca873b0e6bd733938a73f957471a75c.pdf*.

Engagement and Resilience.[195] On the other hand, Kosovo's* definition of "radicalism" in its *Strategy on Prevention of Violent Extremism and Radicalisation Leading to Terrorism 2015 - 2020* is narrower referring to "the process of approving extremist religious beliefs and in some cases converting into a violent extremist."[196] The same strategy nonetheless acknowledges a responsibility for "prevention and combating [of] all forms of religious, political and nationalism-based radicalism and extremism."[197]

Online radicalisation is addressed to a greater or lesser extent in all four of the above-mentioned strategies albeit none of them actually supply a definition. A scholarly definition that fits with the ideas contained in the WB6 strategies, and has been utilised by others, is the description of online radicalisation as "a process whereby individuals through their online interactions and exposures to various types of internet content, come to view violence as a legitimate method of solving social and political conflicts."[198]

The lack of a definition notwithstanding, the role of the Internet in contemporary radicalisation and recruitment processes is addressed on the very first page of Montenegro's *Countering Violent Extremism Strategy 2016 - 2018*, where it is stated that:

> Radicalization of the population of European countries, through the extremist propaganda, is becoming increasingly common, and in the recruitment process modern technological and communication achievements and social networks are used to the maximum extent. Terrorist organizations and extremists exploit technological progress in order to find new ways to engage the dissatisfied, using social networks, video channels on the Internet and radical chat rooms on the Internet.

195 Government of Montenegro (2016). *Countering Violent Extremism Strategy, 2016 - 2018*. Podgorica, p.11. *http://www.pravda.gov.me/ResourceManager/FileDownload.aspx?rid=258024&rType=2&file=Countering%20violent%20extremism%20strategy%202016-2018.docx*.

196 Office of the Prime Minister, Kosovo* (2015). *Strategy on Prevention of Violent Extremism and Radicalisation Leading to Terrorism 2015 - 2020*. Prishtina, p.8: *https://www.peacefare.net/wp-content/uploads/2016/05/Kosovo-CVE-STRATEGY-ENG.docx*.

197 Government of Kosovo* (2015). *Strategy on Prevention of Violent Extremism and Radicalisation*, Prishtina, p.9. *http://www.kryeministri-ks.net/repository/docs/STRATEGY_parandalim_-_ENG.pdf*.

198 Bermingham, A., Conway, M., McInerney, L., O'Hare, N. and Smeaton, A.F. 'Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation'. Paper presented at the Advances in Social Networks Analysis and Mining Conference, Athens, Greece, 20-22 July, 2009: *https://ieeexplore.ieee.org/document/5231878*.

As a result of this aggressive process of attracting new supporters, the phenomenon of "foreign fighters" was created.[199]

Kosovo's* national strategy also has a short section devoted to 'Online radicalisation,' which reads as follows:

> In a time when the Internet plays an important role in human information, it is likely the radicalization to be developed online. In the world of social media such as YouTube, Skype, Facebook, tweeter [*sic*] and many other networks used for general communication, recruiting and influencing the certain views is possible. Currently, ISIS has been effective in providing online space to discuss and perfect their message and seek recruits effectively.
>
> Radical or extremist communities and the accounts can be found on Twitter or Facebook, and provide effective platforms to recruit and manage individuals. But to what extent this is effective it is difficult to say, however, radicalization on the Internet serves as a tool to support a radicalization process that takes place between friends and personal contacts with unknown persons to join the same ideology.
>
> Ordinary people in Kosovo* have visited these sites and posted extremist contents from their behalf.[200]

In terms of the debate on the importance of the role of the Internet, particularly social media, in contemporary radicalisation processes,[201] the Montenegro's and Kosovo's* strategies reflect the opposite ends of the spectrum, with the others somewhere in the middle. This is not uncommon. Some scholars, policymakers, and others view the Internet as an integral component of most contemporary radicalisation processes, especially that of IS. Others are more sceptical however, pointing out that the role of the Internet in radicalisation may be overstated. Many however probably agree with Winter who, when discussing IS propaganda, stated it is not (generally) "singularly responsible for radicalizing individuals, let alone their joining the jihadist cause abroad or carrying out attacks at home… [but] it does catalyse the Islamist extremist's passage from tacit supporter to active member."[202] As a result,

199 Government of Montenegro (2016). *Countering Violent Extremism Strategy, 2016 - 2018*, p.11.

200 Government of Kosovo* (2015). *Strategy on Prevention of Violent Extremism and Radicalisation*, pp.'s 14-15.

201 Conway (2016). 'Determining the Role of the Internet in Violent Extremism and Terrorism', pp.'s 79-80.

202 Charlie Winter. 2015. *The Virtual Caliphate: Understanding the Islamic State's Propaganda Strategy*. London: Quilliam, p.6.

most CVE strategies have multiple areas of focus. The strategies across the WB6 are no different.

For example, the CVE strategy of Albania has four strategic objectives, the fourth of which specifically states "reduce the impact of violent extremist propaganda and recruitment online by using social media to develop and disseminate alternative positive messages".[203] It also aims to counter extremist propaganda while promoting democratic values. It states

The Government of Albania intends to challenge the violent extremist narrative, particularly its transmission via online campaign materials and messages. With respect to this priority area, the Albanian National Strategy puts forth a two-pronged approach to discredit, and in turn mitigate the influence of, extremist propaganda.

First, the Government will improve communication with the public to raise awareness of radicalization and its associated threats. Through clear and effective communication channels, both online and offline, using credible voices such as community leaders, religious authorities, and other role models, the Government seeks to facilitate public discourse, empower local communities with information, dispel myths, and provide answers to the various concerns related to violent extremism. These efforts will serve to dissociate violent extremism from any particular religious group, emphasizing Albania's rich cultural heritage and history of religious tolerance. By providing the public with information on the Government's CVE efforts, this communication plan will increase transparency as well as elicit support and confidence among at-risk groups and the population in general. Second, carefully crafted and contextualized messages and campaigns will be created to counter violent extremist propaganda online, using channels and methods most likely to reach and influence at-risk groups and individuals.[204]

Vurmo (2018) in his report on Albania, as mentioned previously, reported that "the 2015 adoption of the National CVE Strategy and action plan, the increased awareness and engagement of the Albanian Muslim Community (AMC) as well as numerous civil society initiatives to prevent violent extremism, have all contributed to keeping the violent extremist risks under control over the past two and a half years".[205]

The Kosovo* CVE strategy has also identified a number of key objectives of which two relate specifically to online activities. The first relates to early identification of causes, factors, target groups and radical methods. In the regard, the strategy states

In the light of identifying the factors that influence the radicalization, additional activities will be undertaken in cooperation with community, religious communities, and by the state institutions in order to identify the persons and organizations that influence the radicalization of the population, identifying sites / facilities where these extremist or radical ideas are developed; identification of literature that is considered radical and extremist, identifying the websites on the internet which propagate radical / extremist ideas. In relation to identifying the causes of radicalization, emphasize will be paid by interviewing the arrested persons or persons returning from conflict, measurement of the perception of the citizens etc.[206]

Secondly and in relation to prevention of violent extremism and radicalism, the strategy outlines the need for "establishment of team/commission to review the religious content in the internet and if necessary, to engage translators to translate moderated religious content accessible in the internet in Albanian language."[207] However, the State Department report that "implementation [of the strategy] has been uneven across government ministries and a lack of capacity and inadequate resources remained challenges".[208]

Similarly, the CVE strategy of Montenegro identified four cross-cutting issues that must be addressed, one of which relates specifically to Information and Communication Technology (ICT). It notes

The effort to ensure adequate and innovative use of ICT, technology companies and ICT experts at all stages, and through successful CVE activities must include, but should not be limited to, the removal of content or blocking the contents on social media and internet portals that promote violent extremism. ICT should also be utilized to improve the effectiveness of direct responses to extremism, collaboration and coordination amongst CVE actors, as well as the collection of data on extremism and the impact of CVE activities.[209]

To do this, the strategy identifies a number of concrete activities that will ensue implementation of the strategy, a number of which refer specifically to the internet. For example, in relation to activity 1, which relates to adequately understanding of drivers of radicalisation in order to prevent radicalisation, the strategy specifically highlights the need for close cooperation with civil society and the private sector in order to identify threats from the Internet. In relation to activity 2, which relates to the establishment of effective coordination mechanisms among relevant institutions at the national and international level, the strategy states the need to:

Establish national-local partnerships: further coordinate involvement of municipalities in counter-extremism work – through signing a MoU with Union of Municipalities of Montenegro. Establish or designate an Internet Referral Unit: a) coordinate and share the identification tasks (flagging) of terrorist and violent extremist online content with relevant partners, b) carry out and support referrals quickly, efficiently and effectively, in close cooperation with the industry and c) support competent authorities, by providing strategic analysis and operational analysis.[210]

Ensure technology companies and ICT experts are included in the network and set up a working group in this area to develop innovative approaches to the use of technology, internet and social media in tackling violent extremism. [211]

Although an associated Action Plan was developed for the strategy, Bećirević et al. (2018) reported that officials had admitted that they found it difficult to implement the initiatives it envisioned.[212] Others also note issues with the strategy's implementation, such the Centre for Democratic Transition, which claimed that "27 law enforcement agencies were tasked with implementation measures but almost all failed to fulfil their obligations".[213] Bećirević et al. (2018) also found that "some interviewees who noted that a key problem with the Strategy was how loosely it defined responsibilities for its implementation".[214]

Taking a slightly different approach, The Former Yugoslav Republic of Macedonia CVE strategy references online radicalisation in relation to the work of the National Committee for Countering Violent Extremism and Countering Terrorism (NCCVECT). The NCCVEST was established in August 2017 to oversee (non) state (institutional) capacities in their efforts to CVE and terrorism. At the municipal/local level the NCCVECT highlights several areas where national and local authorities should cooperate in this area, one of which includes "refining the comprehensive training and support for religious communities to counter online radicalization".[215] However, according to the State Department reports on terrorism, "the government failed to provide funding to implement this plan".[216]

As mentioned above Bosnia and Herzegovina and Serbia have no dedicated CVE strategy, but they both mention the internet in their counter terrorism strategies. For example, the BiH strategy highlights the need for "special preventive measures [which] foresee combating misuse of the Internet for terrorist purposes, as well as the widespread hate speech and incitement to hate crimes and discrimination".[217] More specifically, it states that

Measures foreseen in the field of investigation and criminal prosecution are focused primarily on further building and strengthening of legislative and institutional capacities of intelligence and security, police and judicial sectors. The main objective of these measures is early detection of terrorist plans and activities, and prompt repressive actions against individuals, groups and networks that demonstrate terrorist intentions. In addition, a special focus of investigative and repressive activities will be put in the following areas: terrorist propaganda and incitement (especially via the Internet), recruitment for terrorist activities, terrorist financing, giving any kind of support to terrorists, and giving instructions or making available any means to terrorists

203 Republic of Albania (n.d.). *Albanian National Strategy Countering Violent Extremism (Unofficial Translation)*, p. 7.

204 Republic of Albania (n.d.). *Albanian National Strategy Countering Violent Extremism* (Unofficial Translation), p. 12.

205 Vurmo (2018). *Extremism Research Forum: Albania Report*, p. 7.

206 Government of Kosovo* (2015). *Strategy on Prevention of Violent Extremism and Radicalisation*, p. 19.

207 Government of Kosovo* (2015). *Strategy on Prevention of Violent Extremism and Radicalisation*, p. 20.

208 See Balkan Insider Website, State Department Balkan Country Reports on Terrorism, 23/09/2018, *https://www.balkaninsider.com/state-department-balkan-country-reports-on-terrorism/*

209 Government of Montenegro (2016). *Countering Violent Extremism Strategy, 2016 - 2018*, p.7.

210 Government of Montenegro (2016). *Countering Violent Extremism Strategy, 2016 - 2018*, p.9.

211 Government of Montenegro (2016). *Countering Violent Extremism Strategy, 2016 - 2018*, p.9.

212 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.6.

213 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.24.

214 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.24.

215 Government of [The Former Yugoslav Republic of Macedonia] (2018). *National Committee for Countering Violent Extremism and Countering Terrorism*, 2018 – 2022, p. 16.

216 See Balkan Insider Website, State Department Balkan Country Reports on Terrorism, 23/09/2018, *https://www.balkaninsider.com/state-department-balkan-country-reports-on-terrorism/*

217 Government of Bosnia Herzegovina (2015). *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism, 2015-2020*, p.9.

that can be used for the commission of crimes of terrorism. [218]

By using the available investigative activities and special investigative actions, and introducing new elements of the Criminal Procedure Codes (in order to effectively fight the planning of terrorist activities and actions), track communication channels of terrorists, and prevent the spread of terrorism knowledge, especially through the Internet. [219]

One key action of note also worth highlighting in this strategy, aligning it to the cyber security strategy, is the reference to CERT. It recognises the need for "full implementation of international standards in the field of cyber security in particular those relating to the establishment of CSIRT in BiH and mechanisms for monitoring and combating the misuse of the Internet for terrorist purposes". [220] This is not evident in the other strategies of the WB6 economies.

The Strategy on Prevention and Countering Terrorism in Serbia has also identified several strategic objectives, in four priority areas: Prevention, Protection, Prosecution and Response. Under the first priority area, prevention, the strategy sets out the role of the internet in relation to its objective relating to developing skills relating to strategic communication. This specific sections states

Developing strategic communication, including confronting malicious interpretation of religious teaching and extremist messages in the public media and on the internet will enable consistent policy of communication with the public at the national level, ensure the promotion of alternative, positive messages, and improve the approach to revealing illegal contents on the internet which publicly justify terrorism.

This objective will be achieved through the efforts to recognize the importance and advantage of the skill of strategic communication at the level of preventing violent extremism and radicalisation leading to terrorism, and to build the necessary capacities for its implementation.[221]

It also sets out an action to "define and develop the system for monitoring and restricting illegal contents posted on the internet, relating to violent extremism and radicalisation leading to terrorism, in accordance with the right to the freedom of expression and privacy".[222] Critics have pointed out that this strategy "makes no mention of right-wing extremism and foreign fighters that fought in Ukraine whatsoever, despite the fact that many Serbian think-tanks, and experts criticised this step and recommended that Serbian nationalist extremism should be included by working group drafting the Strategy".[223] With one interviewee reported as saying "It is obvious that all Serbian governments are fine with right-wing extremists using them for different shady jobs". [224]

Each economy appears to take a different perspective in this regard, with none fully harmonised with the EU strategy. That said, the presence of strategies is positive, but more could be done to enhance the current strategies at place in the WB6 at present to ensure greater alignment with the EU strategy and across the WB6 economies. Furthermore, greater complementarity between these strategies and cyber security strategies would also be beneficial.

4.2 Regional Activities

It is not possible to mentioned all regional activities in this this area, but one important activity is worth mentioning, and that the work of the Integrative Internal Security Governance (IISG). IISG is

a new approach to internal security governance capacity-building and reform introduced in the Western Balkan region. The concept enables a coordinated, aligned and sustainable effort in the major fields of internal security governance reform on part of the EU and all relevant international donors of external assistance.[225]

IISG aims to improve the governance and efficiency of internal security cooperation in the Western Balkan region via three pillars, namely, the Western Balkan Counter-Terrorism initiative (WBCTi), the Western Balkan Counter Serious Crime initiative (WBCSi) and the Western Balkan Border Security initiative (WBBSi). The work of the WBCTi is what is most pertinent here. It is an EU-supported effort to respond to the developments related to Terrorism, Violent Extremism and Radicalisation phenomena in the Western Balkans by maximizing the potential of Regional Cooperation policy and by merging the efforts of all relevant security actors in this area of policy development in an efficient – and sustainable – manner.[226]

Since April 2017, the WBCTi have been implementing 'Support to Prevention and Countering Violent Extremism (P/CVE) in the Western Balkans'[227], which will continue until September 2019. This regional action, funded by the EU instrument IPA II 2016, will contribute to sustainable regional cooperation efforts in the Western Balkans in the area of CT, P/CVE, dealing with phenomena of FTFs and radicalization in the designated period. The action will assist the WB [economies] in their efforts by transferring EU good practices and standards. It will further support the setting up of a national inter-ministerial P/CVE platform in each WB [economy], mirrored by multi-agency co-ordination arrangements at the local level to ensure a top-down and bottom-up approach to P/CVE as well as it will represent a solid and sustainable ground for P/CVE national capacities. Furthermore, the action will provide support to several small-scale actions.[228]

The project is coordinated by DCAF Ljubljana, and the implementation partners are the Regional Cooperation Council (RCC) Sarajevo, the United Nations Development Programme (UNDP), and the International Organization for Migration (IOM).

Further to that, some excellent research is being done in this area within the WB6. For example, the Kosovo* Centre for Security Studies (KCSS) conducted an in-depth piece of work into online extremist content in the Albanian language, which was funded through an EU project. This report was referenced in section 2 when discussing the prevalence of extremist content in the WB6. Similarly the British Council, through the Western Balkans Research Forum has supported researchers to look at the issue to provide a better understanding in this area so the United Kingdom and WB6 partners can better address radicalisation. This research was conducted across all WB6 economies and was funded by the UK. Such organisations have also conducted significant work in evaluating the CVE strategies across the WB6. Some of these were referenced in the report, however, unfortunately it is beyond the scope of this study to go into this and the work of similar organisations in more depth.

Similar as in the case of cyber security, the presence of these strategies, legislation and initiatives should not, of course, be viewed as indicative of significant progress in the area of online radicalisation. While these developments are positive, more needs to be done. This is evident from the 2018 EU assessments of the WB6 carried out by the European Commission (see Table 1). Despite reference to progress in the area of CVE, there is limited specific reference in any of the WB6 assessments of online radicalisations. For example, in the case of Albania, the assessment notes that such content is increasing in Albania and as a result recommends the government increase efforts to make the National Centre for Countering Violent Extremism fully operational.

218 Government of Bosnia Herzegovina (2015). *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism, 2015-2020*. pp.'s 10-11.

219 Government of Bosnia Herzegovina (2015). *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism, 2015-2020*, p.21.

220 Government of Bosnia Herzegovina (2015). *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism, 2015-2020*, p.10.

221 Government of Serbia (2017). *National Strategy for the Prevention and Countering of Terrorism, 2017-2021*, p. 6.

222 Government of Serbia (2017). *National Strategy for the Prevention and Countering of Terrorism, 2017-2021*, p. 11.

223 Petrović and Stakić. (2018). *Extremism Research Forum: Serbia Report*, p.35.

224 Petrović and Stakić. (2018). *Extremism Research Forum: Serbia Report*, p.35.

225 See IISG Website, *http://wb-iisg.com/*.

226 See WBCTi Website, *http://wbcti.wb-iisg.com/*.

227 The project is coordinated by DCAF Ljubljana, and the implementation partners are the Regional Cooperation Council (RCC) Sarajevo, the United Nations Development Programme (UNDP), and the International Organization for Migration (IOM).

228 See WBCTi Website, *http://wb-iisg.com/event/support-to-prevention-and-countering-violent-extremism-p-cve-in-the-western-balkans/*.

Table 1. EU Assessments 2018 relating to online radicalisation and extremism	
ALBANIA	The report acknowledges Albania's national strategy to counter violent extremism (CVE), noting its reference to countering extremist propaganda. It also makes reference to the 2016 appointment of a national coordinator for CVE. It noted that online radicalisation content in Albania is on the rise and as a result recommends that the government steps up efforts to counter external influences that could lead to further radicalisation and to make the National Centre for Countering Violent Extremism fully operational with adequate funding and staff.[a]
BOSNIA AND HERZEGOVINA	The report refers to an EU Senior Mission on counter terrorism and prevention of violent extremism that took place in April 2017. It noted that this assessment made several recommendations, such as the implementation of the strategic framework and internal coordination, in particular in the area of prevention of violent extremism.[b]
KOSOVO*	The assessment acknowledged the existence of a strategy on the prevention of violent extremism and radicalisation leading to terrorism, which has been in place since 2015, noting that 61% of the activities in the action plan were implemented and 14% of the activities were partially implemented. It also recognised that "the government and Technical Working Group for the Prevention of Violent Extremism meet on regular basis thus ensuring cooperation between authorities and other actors, including civil society and religious communities". Despite this, the assessment assessed that the authorities continue to be faced with the challenge of violent extremism and radicalisation, partly due to the presence of violent extremist groups using social media to spread propaganda and recruit followers. The assessment recommended that Kosovo* should increase its efforts to counter these messages.[c]
MONTENEGRO	The assessment acknowledged the new national Serious and Organised Crime Threat Assessment which was adopted in December 2017. This identified terrorism and religious extremism as one of its priority areas. It also acknowledged that the implementation of the 2016-2018 strategy to combat violent extremism was delayed due to insufficient capacity and resources. It further noted that "despite the relatively low visibility of the terrorist threat in Montenegro, especially relating to radicalisation and the return of foreign fighters, institutional awareness needs to be increased to monitor possible terrorist threats".[d]
SERBIA	Serbia's legal and policy framework is largely aligned with the acquis and international instruments on anti-terrorism. The new Law Amending the Law on the Freezing of Assets for the Purpose of Terrorism Prevention was adopted in December 2017. The national strategy and action plan for preventing and fighting terrorism (2017-2021) was adopted in October 2017. It covers prevention of violent extremism and radicalisation, elimination of terrorist threats, and response and prosecution in the event of terrorist attacks. The assessment notes that cooperation between the Police Service for Combating Terrorism and Extremism and Europol intensified in 2017 and is at a very good level. It also noted that there is progress with prevention and anti-radicalisation activities, involving local religious leaders, local authorities and civil society through targeted activities with the OSCE mission to Serbia.[e]
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA	The assessment noted that all necessary measures were adopted to prevent and fight terrorism. Specific actions include the appointment of the National Coordinator for Counter-Terrorism and Countering Violent Extremism. The National Committee for the Prevention of Violent Extremism and the Fight against Terrorism was also created, which is headed by the National Coordinator. However, the assessment noted that there are no prevention and anti-radicalisation measures. Furthermore, whilst the assessment noted that the legal framework on hate speech is generally in line with international standards, its implementation needs to be improved as online hate speech remains unregulated.[f]

Sources [a] European Commission Staff (2018). *Albania 2018 Report*, Strasbourg, 17 April, p. 24: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-albania-report.pdf.*; [b] European Commission Staff (2018). *Bosnia and Herzegovina 2018 Report*, Strasbourg, 17 April, p. 23: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-bosnia-and-herzegovina-report.pdf*; [c] European Commission Staff (2018). *Kosovo* 2018 Report*, Strasbourg, 17 April, p.29: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-kosovo-report.pdf*; [d] European Commission Staff (2018). *Montenegro 2018 Report*, Strasbourg, 17 April, p. 29-31: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-montenegro-report.pdf; [e] European Commission Staff (2018). *Serbia 2018 Report*, Strasbourg, 17 April, p.63: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-serbia-report.pdf*; [f] European Commission Staff (2018). *The Former Yugoslav Republic of Macedonia 2018 Report*, Strasbourg, 17 April, p. 33: *https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-the-former-yugoslav-republic-of-macedonia-report.pdf*.

4.3 Challenges to operational implementation

There is concern amongst policy makers, police, prosecutors and others across the WB6 regarding the role of the internet in radicalisation processes. Particular apprehension was reserved for IS fighters' social media activity and official IS online content targeting the region, particularly in regional languages, acting as drivers of radicalisation. IS's loss of territory, the targeting of its media leaders, the decline in its online content output, and the disruption by major social media platforms of the latter's dissemination means that the levels of apprehension reached in the 2014 – 2017 period have been considerably reduced. However, concerns still exist and while strategies and legislation do exist, the lack of progress in operationalising the strategies was highlighted throughout much of the field research. These challenges, for the most part, were consistent with those found in respect to cyber security, and included issues such as (i) limited resourcing of bodies, such as police, and prosecutors in respect of staffing, technology, and training, which is negatively impacting investigations and procedure; (ii) limited appropriate civil society participation; (iii) the lack of significant public-private partnerships; (iv) the lack of educational policies and programmes on identifying risky online content; and (v) the need for more careful media reporting. These findings were consistent, for the most part, with other evaluations of this nature as mentioned in brief above. These will be discussed in the next section, but before that the report briefly discusses the official response to online radicalisation.

4.3.1 Operational Responses

The police are responsible, for the most part, with the cooperation of prosecutors, for responding to extremist content, radicalising content, and recruitment material, both online and offline. Progress albeit slow has been made by police. Officers and prosecutors tasked in this area are deemed to be very proficient, with many of them having received extensive training and having extensive technical knowhow. However, as with cyber security, these units complain of high workloads and lack of proper resourcing, financially and in terms of staffing. In fact, the police resources in this area are modest in all respects and therefore units cannot work at the level required of them. Training received both at home and abroad has helped, but cannot replace the need for increased technology and staffing.

Specialised units have been established in this area throughout the region. For example, a dedicated unit was established in Serbia's Ministry of Interior to deal with terrorism and extremism. However, this unit reportedly suffers from a lack of adequate resources, in the form of manpower, specialised training, and financing. Interestingly, while this specialised unit is dedicated to terrorism and online radicalisation, a different unit is tasked in relation to other forms of cybercrime. This is the case elsewhere in the WB6 too. For example, in Montenegro the Special Police investigate cases relating to terrorism and violent extremism and deal directly with the Special Prosecution's Office. [229] They also deal with gang related homicides, corruption, and other serious crimes[230], while, as mentioned above, a dedicated unit for High Tech Crime is responsible for investigating crimes that entail any element of cyber. Little overlap between the two units means there is negligible cross-transfer of experience and knowledge. This limits, for example, knowledge sharing on emerging patterns of criminal behaviour online, new tools and technologies and their use by online criminal networks, etc.

None the less, positive examples of progress are evident in other areas of the police. For example, improvements have been made to increase the competency of the community police to respond in this area. This is in line with the EU Strategy, which notes that community police officers need to be trained to help counter radicalisation. The Albanian Strategy approach echoes this sentiment, for example, by introducing a community policing model into the economy to ensure the delivery of this commitment. Interestingly, the Strategy of The Former Yugoslav Republic of Macedonia notes similar

229 RB23 interviewed between 17 and 19 June 2018 in Podgorica

230 RB23 interviewed between 17 and 19 June 2018 in Podgorica

needs, whilst also acknowledging in a SWOT analysis that 'weak trust-bonds between local police/law enforcement authorities and local persons' exist at the municipal level, which they note need to be addressed.[231] The strategy from Kosovo* also mentions the need to build trust with the community, while the Serbian Strategy notes the need to build public trust in the judicial system's ability to response to such offences.

4.3.2 Investigations and prosecutions

At the operational level, police and prosecutors highlight the fact that it can be difficult to have violent extremist online content removed and when it is removed, it is often uploaded again on another site within hours or even minutes. Also noted was the difficultly of tracing the origin of content and those responsible for creating it, highlighting the borderless aspect of this content, as already discussed. Acknowledged too was that it is sometimes difficult to assess the content. For example, identifying more hard-line content as extremist is generally straightforward, but some of the softer content is less indicative. For example, the type and nature of content produced and circulated by religious ideological extremists has evolved over the past four to five years, it was said.[232] This changed from quite a hard-line approach to recruitment within content targeting the region to a softer approach that presents a more rational explanation of injustices, oppression, and religion, [233] with the 'soft' content being much more difficult to identify and deal with. As a result, much of the latter remains live and accessible. This softer approach was described as being used to attract more sympathisers and spread influence amongst the masses[234] and, crucially, being reinforced by 'real world' social support structures that are developing at grass roots level, where state services are not being implemented or are not accessible.[235] These groups are thus capitalising on feelings in communities of frustration, lack of trust, deprivation, and an environment of political corruption.[236]

Despite this, as mentioned earlier in the case of The Former Yugoslav Republic of Macedonia, police and prosecutors have used online content as evidence in criminal cases, including securing convictions for online recruitment, illustrating a level of competence and success in this area. Worth noting here is that experience in prosecuting such cases could be useful for police, prosecutors, and judges dealing with other types of cybercrime, given many complained that they were not getting enough experience of such cases. Bećirević et al. (2018) found in the case of Montenegro that the police see the responsibility in this area lying with other agencies, as well as the police noting that "a police respondent also stressed the importance of an interdisciplinary approach, saying that police agencies cannot be expected to bear the burden of prevention alone". [The police man stated] "This is a problem for all of society, and a partnership between the state and civil society is crucial".[237]

4.3.3 Civil Society

The EU Strategy identifies a number of responses as noted above, one of which is to support individuals and civil society to build resilience. Similar to their cyber security strategies, all of the WB6's counter-terrorism and CVE strategies recognise a role for civil society. For example, Kosovo's* strategy identifies a number of activities in this area including, with respect to online, cooperation between the community and state institutions to identify persons and organisations engaged in radicalising activity, literature that is considered radical and extremist, and websites that propagate radical/extremist ideas. While the Strategy of BiH states the need for "coordinating response to the increasingly violent and extreme events; strengthening the role of civil society, especially the youth, women, religious leaders and victims of extremism and radicalism that leads to terrorism, through the development of local strategies".[238] However, more needs to be done. For example in the case of Albania, Vurmo (2018) quoted an informant as saying:

It is time that the implementation of the National CVE strategy involves community stakeholders – religious groups, local governments, civil society and others. AMC [Albanian Muslim Society] has been an active player in the past two years and we must support their local clerics and representatives to dismantle peer to peer influence radicalisation of religious believers.[239]

231 Government of [The Former Yugoslav Republic of] Macedonia (2018). *National Counterterrorism Strategy*, p.18.

232 RB22 interviewed between 13 and 16 June 2018 in Belgrade

233 RB22 interviewed between 13 and 16 June 2018 in Belgrade

234 RB22 interviewed between 13 and 16 of June 2018 in Belgrade

235 RB22 interviewed between 13 and 16 June 2018 in Belgrade

236 RB22 interviewed between 13 and 16 June 2018 in Belgrade

237 Bećirević *et al*. 2018. *Extremism Research Forum: Montenegro Report*, p.24.

238 Government of Bosnia Herzegovina (2015). *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism, 2015-2020*, p.6.

239 Vurmo, G. (2018). *Extremism Research Forum: Albania Report*, p.14.

Unlike in the area of cyber security however, there are many CSOs active in CVE and counter-terrorism-related issues within the WB6. In fact, a criticism often made is that there are too many CSOs active in this area, with the further criticism that many of them are driven by money rather than interest and expertise often levelled. Disapproval that many of these CSOs ignore or fail to see the bigger picture in terms of the possible misuse of online content removal practices to censor certain voices was also stated. Similar to the area of cyber security, there is a need to attract more CSOs into the debate that can engage on the latter topic and related issues to ensure any actions taken are justified due to risk of serious crime, while remaining respectful of human rights, privacy, freedom of information, and media freedom. The need to respect human right is central to both the EU strategy in this area, but also in relation to the cyber security, and is a sentiment echoed within the strategies of the WB6.

4.3.4 Public-Private Partnerships

The EU Strategy highlights the need for public-private partnerships in this area, a key component also noted in relation to cyber security. The Strategy states that

The use of the internet and social media is critically important, not least to respond promptly to online rhetoric supporting terrorism and to reach those most vulnerable to radicalising messages. In this regard, public-private partnership should be encouraged to tackle the challenge of radicalisation online.[240]

Interestingly, whilst all the strategies mooted the role of the private sector and consistent with the strategies on cyber security, such cooperation was identified as important, these relationships are inconsistent, resulting in different levels of response across organisations. Where relationships are good and joined-up thinking occurs, responses can be swift and effective, but where they are not, a lot of time and resources may be wasted. Making improvements in this area has particular relevance in the area of online radicalisation, given that the majority of ISPs are private companies, but additional to that, their positive impact can have significant impact, as presented in section 3. As things stand, developing such relationships can be negatively impacted by existing processes. For example, different response protocols often exist within ISPs and other service providers for cases of cybercrime and counter-terrorism, often with extra layers of bureaucracy added, resulting in the need for multiple Memoranda of Understanding (MOUs) with the same organisation. This is not conducive to developing productive and flexible partnerships. The lack of tradition of public-private partnerships within the WB6, as mentioned in volume 1, may be hindering the development of such approaches, rather than an unwillingness to develop such relationship, as the majority of people interviewed recognised the value of such relationships.

4.3.3 Education

Education is an important component in the EU strategy. If of poor quality, it may be a factor that makes some more vulnerable to radicalisation and recruitment to terrorism. As a result, the EU strategy states that education must be strengthened "to enable opportunities and critical thinking, and promoting tolerance and mutual respect, exchanging viewpoints and communicating to civil society the success in these areas".[241] It further notes that education need not be exclusively or explicitly relating to countering radicalisation and terrorism, that improvements in the education system is in itself a positive thing, noting that work is significant and valuable in its own right. For example, the strategy highlights the importance of education in the context of building resilience and to recognise the dangers of terrorist narratives. All the strategies recognise the role of education in this area. The Albanian Strategy explicitly refers to critical thinking through education, and is rolling this out through the 'School as a Community Center'. During the interviews many noted that while progress is being made in this area, more needs to be done to access hard to reach groups and individuals.

4.3.4 Media

Unlike the EU Cyber Security Strategy, which did not specifically mention the media, the EU Strategy on Countering Violent Extremism does. It states

We should support and amplify counter-narratives emanating from those with local influence, including community leaders where this concept applies, teachers, families, youth workers, public figures, thinkers, scholars, academics, religious leaders, businesspeople, media personalities, singers, sports stars and others who lead or shape public opinion and who can tell a positive and credible story. We

240 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p. 8.

241 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p. 6.

should initiate projects with these actors at all levels and work to ensure that they are appropriately empowered and supported.[242]

All the strategies reiterate the necessity to have strong relationships with the media, viewing the media as key stakeholders in countering violent extremism. That said, how this plays out on the ground has yet to fully materialise. Criticisms made during the field research note that many media outlets do not appear to understand how to report such stories properly, often just recirculating content to support their story. Furthermore, given existing tensions within the region, some note that there can be a lack of maturity in reporting, often reported in a manner to support a vested interest rather than to objectively reporting the news.

That said, some progress has been achieved in this area. For example, KCSS published a Journalists' guide - Violent Extremism: Definition and Terminology in May this year. The guide was produced in cooperation with Kosovo* media. It was done so [in] "the absence of a compendium of the terminology and practices, in order [for journalists] to properly respond to the need for more accurate and substantive surveys and reporting on the phenomenon of violent extremism in Kosovo"*.[243] KCSS, through the guide, aimed to build on positive existing relationships between Kosovo's* media, researchers and civil society with the objective of "push[ing] forward a progressive agenda that focuses its efforts on the democratization of the public sphere and the promotion of a genuine debate on informing Kosovo* citizens as accurately as possible".[244] Furthermore,

Despite being primarily intended for use by the media, this guide is an initial effort to harmonize the knowledge on violent extremism and to clarify a host of issues pertaining to this phenomenon. It is also intended for use by Kosovo* institutions, non-governmental organizations, research institutes, analysts and commentators, and all researchers seeking basic knowledge on violent extremism. In addition, this guide provides an overview of the background and main established facts on violent extremism in Kosovo,* an overview of the legal aspects related to tackling this phenomenon, some international media practices on reporting on specific terrorist groups and terrorist attacks, and a glossary of over 7,000 words employed in the propaganda effort of the Islamic State terrorist organization, which have not been previously used in Kosovo,* in order to increase the media's awareness of the usages of these words or terms in their reports.[245]

A second such example is the recent handbook for journalists, titled Terrorism and the Media, launched by UNESCO. This handbook was "designed to help [media] carry out their work informing the public while avoiding the risk of actually helping terrorists achieve their aim of dividing societies and turning people against each other" and "aims to raise journalists' awareness of the need to exercise caution and examine carefully who they quote, what messages they relay and how they contextualize the information they give, despite the pressures to win readers, viewers and listeners".[246]

However, the problems may not solely reside with the media themselves, some report that it can be difficult to get access to accurate information from law enforcement, politicians and other government organisations to validate or support their stories, or to challenge dis-information. Furthermore, a number of media organisations reported that they had been the victims of cyberattacks, ranging from basic to sophisticated. This resulted from their reporting on, addressing, and/or hosting content or events objected to by some extremist individuals or groups. This is evidence that some extremist groups and/or their sympathisers have the capacity and skills to conduct a range of cyberattacks if desired. However, in a similar way to the private sector, these organisations said they rarely report such attacks, given they believe that it is highly unlikely that any action will be taken. Many noted that when they report extremist content or hate speech, limited responses are received, for the most part, with the content staying live in the majority of cases. The most they reported doing was conducting post-mortem analyses themselves so they could take remedial action to protect against them in the future. Some also reported that they conduct analyses to try to determine from whom and where attacks originated. Such knowledge, they said, could also be useful for ongoing or future stories.

4.3.5 Other challenges

It is evident from the findings in relation to online radicalisation and extremism that similar challenges exist as do in relation to cyber security. Resourcing, both financially and staffing, coupled with lack of technology appear to hinder the work of the police in this regard. Coupled with that, despite the acknowledgment to work more closely with the private sector, civil society and others in this area, this has yet to adequately materialise and requires further commitment and efforts. Furthermore, despite the clear synergies between cyber security and online radicalisations and extremism, the majority of the strategies do not clearly articulate this link. In fact, the Strategy of Bosnia and Herzegovina is the only one to mention CSIRTs explicitly, as mentioned above. It is clear that awareness raising needs to be conducted in this regard to heighten policy makers and practitioners in this area of the synergies between online radicalisations, online extremist content and cyber security. Nonetheless, progress is being made and there does appear to be a willingness to continue to improve capacity and capabilities in this regard.

Other challenges in this area relate to cooperation, at the local, regional and international level. Locally, cooperation between units dealing with cybercrimes and those dealing with terrorism is not at the level required. The reason for this is two-fold. For one, the system is not structured in a manner that aligns these units closely, as mentioned above. The second reason is more practical, possible overlap between these two areas is not often evident in the early stages of investigations. This lack of active cooperation has a number of drawbacks. Chief amongst these is that if a cyberattack does not have the optics of terrorism from the start, it goes through the procedure of being reported to the national CSIRT and then, if necessary, handed over to police to be investigated as a cybercrime. However, if it is later found to have a terrorism component, it is likely that it would be transferred to counter-terrorism police. This complicates processes and could result in cases falling through the cracks. That said, cooperation in online radicalisation and extremism cases that involve terrorism cases experiences a higher level of cooperation at all levels, locally, regionally, and globally given the importance attributed to it. However, as noted in volume 1, cooperation in relation to cybercrimes is often less effective. Positive lessons of cooperation in relation to cases of online radicalisation and extremism may be transferable into the field of cyber security to enhance cooperation.

4.3.6 Funding

Similar to cyber security, very little documentation could be located on how the WB6 fund or intend to fund future developments in this area, either at regional or economy level. Most of those interviewed noted that a lot depends on donor funds and their programmes.

242 Council of the European Union (2014). *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, p. 8.

243 Perteshi, S. (2018). *Journalists' Guide - Violent Extremism: Definition and Terminology*. Prishtina: Kosovo* Centre for Security Studies: *http://www.qkss.org/repository/docs/Guideline_669605_187367.pdf*.

244 Perteshi (2018). *Journalists' Guide - Violent Extremism: Definition and Terminology*, p.7.

245 Perteshi (2018). *Journalists' Guide - Violent Extremism: Definition and Terminology*, pp.'s 7-8.

246 UNESCO (2018). *Terrorism and the Media: A Handbook for Journalists*. Paris: UNESCO: *https://en.unesco.org/news/terrorism-and-media-handbook-journalists. This document is also available in Bosnian at http://unesdoc.unesco.org/images/0026/002657/265733hbs.pdf*.

5. FINDINGS AND RECOMMENDATIONS

Similar to cyber security, there is significant progress in the WB6 in the area of online radicalisation and extremism, and with respect to harmonisation of legislation and strategies with the EU. However, implementation of some key aspects of the strategies has still not materialised. Similar again to cyber security, challenges in the area of funding, staffing, and technological advancement within government agencies hinder such development. Coupled with this, the limited pace of development in the area of public-private partnerships, educational progress and media awareness also significantly impact the response. None the less, due to work similar to that conducted by KCSS and under the project of the British Council, there is an increasing high level of awareness of the extent and prevalence of online radicalisation and extremist content online and being accessed, developed and circulated within the WB6. This increased level of awareness is important in developing effective responses. That said, it is evident that radicalisation and extremist content is viewed for the most part through the traditional lens of terrorism and violent extremism, and religious extremism at that, within the WB6, a perspective echoed in much of the EU documents and reports. This needs to change given the increased risk of information attacks. Coupled with that, the presence of extreme right wing content, and increasingly nationalistic content, illustrates the need for a greater commitment to looking at these issues from a wider lens.

Furthermore, the need to look at online radicalisation and extremist content through the lens of cyber security was evident in the findings for this report, both within the context of the WB6 and more generally. Firstly, the hosting and distribution of extremist content online takes advantage of the same technology as those used in cyber attacks. Malicious actors use such cyber technologies and infrastructures to target information, weaponising the Internet, particularly social media, to forward their goals. Secondly, both sets of actors are using the borderless nature of the internet to operate, extending their reach, thereby enabling them to circumvent obstacles in their own economies. For example, interviewees in Bosnia and Herzegovina noted that extremist content removed from sites in BiH re-emerged on sites hosted outside of BiH.

As a result, approaching online radicalisation and extremism as a cyber security issue, one that targets information, has its merits. Firstly, such an approach could foster better cooperation and exchange of information at the operational level. Technology could be shared, potentially reducing costs, and expertise could be exchanged, thereby getting the best use of already tight resources. Furthermore, improved internal cooperation could encourage better external cooperation too. But the benefits of viewing online radicalisation as a cyber security issue go beyond this, and looking at it from this perspective may be timely, given increased discourse on so-called fake-news and the potential for a variety of other information entrepreneurs to engage in sophisticated information operations. We need to challenge our contemporary conceptions of cyber security, which largely focus on kinetic attacks and omit online information operations, and critically assess whether this approach remains fit for purpose.

Recommendations

Similar to volume 1, the following recommendations are provided to help address these challenges and to maximise progress in relation to the harmonisation of laws, strategies, and actions plans. Sufficed to say that the recommendations in volume 1 are also applicable in this area. For example, all strategies and action plans relating to countering violent extremism should be resourced effectively. The reporting structures relating to suspect online extremist content should be developed and explained to the necessary stakeholders to ensure consistency in reporting. Furthermore, there is a need to increase awareness on the part of citizens as regards to online extremist content, right to freedoms of speech, surveillance, fake news, extremist content, cyber terrorism, etc. Activities in this area should also be conducted with CSOs, community groups, and private sector providers to ensure a multi-layered approach. Finally, at the national level, economies should maximise and leverage existing expertise and in so doing, help identify and develop PPPs and synergies between stakeholders.

The recommendations at the regional level also hold relevance in relation to online radicalisation and extremism. These include: to develop a more strategic approach to regional cooperation, to realign support of the international community to the strategy of the region, and to establish a regional centre of excellence. All these developments should also include a component relating to online countering violent extremism. This will ensure a more comprehensive approach in this regard, ensuring it is embedded within both a cyber security and CVE/counter terrorism perspective.

5.1 National-level recommendations

Despite progress in each of the WB6 with regard to online radicalisation and extremism, more needs to be done. The following recommendations should assist in achieving this.

5.1.1 Review Countering Violent Extremism Strategies to ensure greater alignment with the EU Strategy for Combating Radicalisation and Recruitment to Terrorism

Only limited alignment was found between the CVE of the four economies with the EU Strategy for Combating Radicalisation and Recruitment to Terrorism. This was in contrast to the cyber security strategies, which were found to be closer aligned. It is recommended that each of these four strategies are reviewed to ensure greater alignment with the EU strategy. It is also recommended that both Bosnia and Herzegovina and Serbia ensure alignment with this policy when they finalise their CVE strategies. Such alignment could start with using shared definitions of key terms, which are absent at present from the strategies, as mentioned above. Introducing shared definitions may make it easier to cooperate across borders. That said, there is no one strategy that fits all contexts, so strategies need to be based on local need first. That said, a consistency and complementarity in approach is recommended.

5.1.2 Review Counter Terrorism and Countering Violent Extremism Strategies to ensure consistency and complementarity with Cyber Security Strategies

To date, and as mentioned previously, countering online violent extremism has largely been viewed through the lens of counter terrorism. However, given the emergence of information based attacks, it is no longer effective to view online radicalisation and extremism solely through this lens. As a result, it is recommended that each economy reviews their counter terrorism and countering violent extremism strategies to ensure their consistency with and complementarity to their cyber security strategies, as is the case with both EU strategies. This will also enable greater alignment at the operation level and better use of resources, if implemented properly. This may involve the need for awareness raising to illustrate the synergies between both areas.

5.1.3 Review Strategies and Legislation in the area of Counter Terrorism to ensure attacks on Information Systems are included

Given the emerging growth of attacks on information systems knowing how to respond will be increasingly important. Therefore, registering of attacks on information systems and empowering law enforcement and prosecutors to have adequate response capabilities in this regard seem to be of crucial importance . This would also ensure greater alignment with EU legislation. For example, as previously stated the EU Counter Terrorism Directive refers to attacks on information systems, alongside physical attacks.

5.1.4 Review current relationships with Private Sector Companies, Civil Society Organisations, and the Media, and develop specific actions to improve the same

Despite recognition of the need for more effective relationships with private sector companies, CSO and the media as outlined in the majority of strategies of the economies of the WB6, this has yet to fully materialise. Therefore, it is recommended that each economy conduct a scoping exercise to identify key organisations in the private sector, civil society, and the media and actively engage with them to develop better shared responses to online radicalisation and extremist content. Furthermore, it is recommended that these activities are included in their actions plans, which would go some way to ensuring that such objectives are achieved. Additionally, if MOU or written protocols are required to support these relationships, it is recommended that one suffice between each organisation to reduce the levels of bureaucracy as reported.

5.1.5 Introduce critical thinking into cyber security education

As noted earlier in the report, education in the area of cyber security at the national, secondary and third level is improving, albeit at a slow place. Nonetheless, such training provides an excellent opportunity to include age appropriate critical thinking training to children and young adults so they learn the skills to critically assess the validity of the information, arguments and authenticity of information put before them. As a result, it is recommended that the WB6 introduce critical thinking components into the education curriculum. This will help create greater societal resilience to future information operations campaigns. Improved critical thinking skills are not just generally desirable, but should cause users to be more critical of extremist and terrorist content, which would be positive.

5.2 Regional-level recommendations

5.2.1 Ensure a consistent approach to extremism and extremist and terrorist online content

It is acknowledged that there is a range of good research already available and currently being conducted on extremism in the WB6, which is positive. A drawback is the almost exclusive focus on violent jihadism, especially IS. Such an approach is likely to skew our understandings of the nature of extremism and radicalisation in the WB6. It is recommended that additional research is conducted that extends beyond jihadist online content, to include extreme right and nationalist content, whilst also being mindful of other emerging extremist content, so a more balanced picture is produced in this regard. This analysis might be best conducted at the regional level given that findings suggest the circulation of online content between economies. This may be best undertaken by the regional centre of excellence recommended in Vol. 1.

5.2.2 Take an intelligence and evidenced based approach

Despite recent setbacks, IS's online footprint remains wide and deep. Thousands of items of high quality IS content are still easily accessible online, including content tailored for WB6 audiences. In some instances, such as that of jihadist Rexhep Memishi from The Former Yugoslav Republic of Macedonia, the online accounts and profiles of imprisoned extremists are maintained and updated by those close to them.[247] Wiping the Internet of all terrorist content is a seemingly impossible task. Nonetheless, making such content increasingly difficult and costly (i.e. in terms of time, know-how, etc.) to locate is a worthwhile pursuit that could be entered into by authorities in partnership with social media and other internet companies. A complementary approach is one driven by intelligence that is also evidence-based. This requires cooperation between law enforcement, tech companies, and ISPs to map networks, identify capabilities, and highlight potential content of interest, be it related to actors, targets, methods, etc. While such an approach may necessitate taking down content, it can be much more targeted to disrupt key relationships.

5.2.3 Develop better relationships with major tech companies

2017 witnessed an increased willingness of major tech companies to restrict dissemination of extremism content. While reputation and economic damage arising from attention to this content was a likely driver, so too was the European Union and some of its Member State governments increased discourse around implementing legislation that restricts such dissemination. This momentum should be maximised within the WB6 and at the economy level. Contacts with major internet companies should be developed to understand how WB6 economies can better work together with them to monitor and respond to extremist content, before having to go down the road of legislative change. Furthermore, WB6 economies should look at building relationships and involvement with forums such as the EU Internet Forum and the Global Internet Forum to Counter Terrorism (GIFCT), with a view to creating a Western Balkans Internet Forum (EUIF) similar in structure and design to the EUIF, but focusing on content produced in Western Balkans languages.

5.2.4 Establish a Western Balkans Referral Unit

Similar to the EU IRU, a Western Balkans referral unit could have significant impact on online content produced in Western Balkan languages. Given that the EU IRU only has limited capacity in these languages, a WB6 version of the EU IRU would be complimentary to the EU IRU and as a result, the EU IRU may be willing to support the development of such a unit.

5.2.5 Develop and adopt a Western Balkans Agenda on Security

To ensure a consistency in approach in relation to online radicalisation and extremism, and in relation to security as a whole, it is recommended that a Western Balkan Agenda on Security be developed and adopted at the regional level. Similar to the Digital Agenda for the Western Balkans, mentioned in Vol. 1, this approach could be used to support a regional approach to security, including online extremism and radicalisation. Having a detailed Agenda based on regional needs would be likely to ensure more structured direction of donor funds, reduce overlap and duplication, and enable the WB6 to maximise the benefits of shared resources.

5.2.6 Develop a Western Balkan version of the Radicalisation Awareness Network

The Radicalisation Awareness Network (RAN) is recognised within the WB6 as an excellent resource for information, expertise, and knowledge sharing at the EU level. Given the wealth of knowledge within the region, a similar network established in the region would be an excellent way to bring together experts, good practice, and advice on problem solving from a regional perspective. It is recommended that advice and support be garnered from the RAN to support this.

247 Azinović, V. (2018). Extremism Research Forum: Understanding Violent Extremism in the Western Balkans., London: British Council, p. 11: *https://www.britishcouncil.rs/sites/default/files/erf_report_western_balkans_2018.pdf*.

Good.

Better.

Regional.

Regional Cooperation Council Secretariat

Trg Bosne i Hercegovine 1/V
71000 Sarajevo, Bosnia and Herzegovina
T +387 33 561 700 **F** +387 33 561 701 **E** rcc@rcc.int

rcc.int RegionalCooperationCouncil rccint RCCSec

RegionalCooperationCouncil