Centar za sigurnosne studije - BIH
Centre for Security Studies - BH

The importance of cybersecurity for Bosnia and Herzegovina Policy recommendations to support BiH's cyber capabilities and international aspirations

2022

Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

The importance of cybersecurity for Bosnia and Herzegovina Policy recommendations to support BiH's cyber capabilities and international aspirations

Author: Nicolò Miotto

Nicolò Miotto is currently pursuing the International Master in Security, Intelligence & Strategic Studies (IMSISS) awarded by a consortium of European universities – University of Glasgow (UK); Dublin City University (Ireland); Charles University in Prague (Czech Republic). He is Adjunct Professor at Università degli Studi Niccolò Cusano (Rome) where he teaches courses on war crimes, crimes against humanity and genocide. His research interests include terrorism and violent extremism, emerging technologies, international law and geopolitics.

April, 2022

These contents represent the views of the author only and is his/her sole responsibility. The Centre for Security Studies does not accept any responsibility for use that may be made of the information it contain.

Acknowledgements

I would like to thank the Centre for Security Studies (CSS) for supporting me in the production of this report. I am particularly grateful to Benjamin Plevljak, the Secretary-General of CSS, for providing me with the opportunity to carry out this study, for his patience, and for his suggestions and feedback. Especially, I would like to thank him for helping me with drafting the questionnaire and for sending it to BiH public institutions.

I would like to thank Sabrina Berberović-Tadić for keeping in touch with BiH public institutions. Finally, I would like to thank Lajla Leko and Sabahudin Harčević for helping me with the translation of the questionnaires' answers.

Table of content

List of abbreviations

ACN – Agenzia per la cybersicurezza nazionale [Agency for National Cybersecurity]

AEPTM – Agency for Education and Professional Training

AFIV – Agency for Forensic and Expert Examinations

BD – Brčko District

BiH – Bosnia and Herzegovina

CBMs – Confidence-building measures

CEPOL – European Union Agency for Law Enforcement Training

CERT – Computer Emergency Response Team

CI – critical infrastructure

CRA – Communication Regulatory Agency

CSIRT – Computer Security Incident Response Team

DCPB – Directorate for Coordination of Police Bodies of Bosnia and Herzegovina

ENISA – European Network and Information Security Agency

EU – European Union

EUROPOL – European Union Agency for Law Enforcement Cooperation

FATF – financial Action Task Force

FBiH – Federation of Bosnia and Herzegovina

GCSCC – Global Cyber Security Capacity Center

GDPR – General Data Protection Regulation

ICTs – information and communication technologies

INTERPOL – International Criminal Police Organisation

ISO – International Organisation for Standardisation

MoD – Ministry of Defence

MoI – Ministry of Interior

MONEYVAL – Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe

NATO – North Atlantic Treaty Organisation

NCAF – National Capabilities Assessment Framework

NCSS – national cybersecurity strategy

NICS – Next-generation Incident Command System

NIS Directive – Network and Information Security Directive

OSCE – Organisation for Security and Co-operation in Europe

PPP – public-private partnership

RFF – Rapid Financing Facility

RRP – Recovery and Resilience Plan

RS – Republic of Srpska

SIPA – State Investigations and Protection Agency

SPC – NATO Science for Peace and Security Programme

UN – United Nations

UNDP – United Nations Development Programme

USAID – United States Agency for International Development

List of tables and figures

Executive summary

Cybersecurity is a fundamental domain for Bosnia and Herzegovina (BiH) as it impacts the country's national security, its economic growth and its international commitments and goals. Despite the importance of cyberspace for the country, BiH lacks a comprehensive approach to cybersecurity, having instead a jeopardised approach which hinders its cybersecurity efforts. The country's cybersecurity capabilities are underdeveloped, exposing governmental bodies, private companies and citizens to potential cyber threats and risks.

Limited cybersecurity capabilities can undermine BiH's efforts to access the EU and NATO as these international organisations require states to respect and adopt specific cybersecurity standards and legislation. Hence, BiH needs to improve its cybersecurity architecture to achieve its international goals. In addition, the country must enhance its cybersecurity to accomplish international obligations deriving from the country's membership of international organisations and its ratification of the Budapest Convention.

Although the country presents embryonic cybersecurity capabilities, BiH public institutions are improving their cybersecurity awareness by providing public employees with workshops, seminars, and training courses on cybersecurity. As of this, international and domestic cooperation represents a pivotal opportunity for BiH to build and enhance its cyber capabilities; intergovernmental organisations, research centres and partner counties are providing BiH public institutions with funds and training opportunities in the field of cybersecurity.

Keywords: *Bosnia and Herzegovina; cybersecurity; cybercrime; cyber awareness; European Union; NATO*

Introduction

Due to its decentralised approach to cybersecurity based on multiple and different institutions and laws addressing cyber-related issues, Bosnia and Herzegovina (BiH) is greatly exposed to cyber-threats and risks.[1] From cyber-attacks to cybercrime, BiH is increasingly facing menaces and dangers originating from the cyber domain,[2] thus necessitating to take actions and measures to further build and strengthen its cybersecurity capabilities and architecture. This call to action has been made by numerous intergovernmental organisations BiH is part of such as the Organisation for Security and Co-operation in Europe (OSCE) which has emphasised the importance of cybersecurity and the necessity to develop confidence-building measures (CBMs) to reduce the risks of conflict.[3]

Although BiH has adopted fundamental domestic and international legislation, its institutions still lack a comprehensive and effective approach to cybersecurity. A well-designed whole-of-society and whole-of-government approach to the cyber domain would provide BiH and its citizens with great benefits and advantages in diverse sectors of society, ranging from the economy to law enforcement. In addition, strengthening BiH's cybersecurity can facilitate the country's access to the European Union (EU) and the North Atlantic Treaty Organisation (NATO), two long-standing strategic objectives BiH aims to pursue. Indeed, access to the EU and NATO requires the adoption of specific laws and policies as well as the harmonisation of domestic legislation with common standards and guidelines concerning cybersecurity.

This paper aims to analyse the importance of cybersecurity for BiH, explore BiH's approach to the cyber domain and provide policy recommendations to strengthen BiH's cybersecurity capabilities. Particular attention has been dedicated to exploring good practices and standards which can help BiH implement effective cybersecurity policies and support the country's international aspirations. BiH can and need to enhance its cyber capabilities to meet its international commitments and achieve its political objectives. As of this, international cooperation with key partners and stakeholders can provide BiH with opportunities to build its cybersecurity architecture.

This paper will first illustrate the methodology adopted, the limitations of the study and the aims and overall purpose of the research. Subsequently, it will provide the main findings which result from the analysis of primary and secondary data. Finally, the analysis will be centred on the policy recommendations the author of this research aims to provide BiH policymakers with. After briefly enumerating the policy recommendations, the paper will thoroughly explore each of them to offer an in-depth and pragmatic analysis, also explaining how each policy recommendation can be enacted. The study will conclude by offering some further considerations on BiH cybersecurity and outlining key points for future research.

[1] Sabina Baraković and Jasmina Baraković Husić, "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina," *Information & Security: An International Journal* 32 (2015): 131–54, https://doi.org/10.11610/isij.3205.

[2] Ibid.

[3] Organisation for Security and Co-operation in Europe Permanent Council, "Osce Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies" (2016), https://www.osce.org/files/f/documents/d/a/227281.pdf.

This research shows that cybersecurity is a pivotal strategic domain for BiH as it impacts multiple sectors of society. However, data testify that BiH presents underdeveloped cyber capabilities and that the country needs to increase its efforts in the cyber domain in order to ensure national security, achieve the international standards needed to access the EU and NATO and respect international obligations. Despite these major gaps, BiH is enhancing its cybersecurity capabilities; key legislation has been adopted and BiH public institutions are participating in training programmes funded and provided by BiH state and non-state partners. Overall, BiH public institutions' cyber awareness is increasing, and cyber capabilities are being strengthened at both the state and sub-state levels. Nonetheless, policymakers need to take further steps to strengthen BiH cybersecurity architecture by developing a comprehensive approach to cyberspace, producing a state level cybersecurity strategy and, potentially, establishing a state agency for cybersecurity.

Methodology, limitations and aims of the study

This research adopts a mixed approach, using both qualitative and quantitative methods. The study results from a two-stage methodological process:

[1] *Desk research and analysis*: Although there is little research on BiH's cybersecurity, some key secondary sources on cybersecurity issues are available online. Especially, the documents released by the government of BiH as well as by international organisations BiH is part of have been pivotal elements to inform the analysis. Furthermore, the analysis relied upon the small but prominent academic research on BiH's cybersecurity and cybersecurity in the Western Balkans.

[2] *Questionnaire*: A questionnaire (see annex A) concerning cybersecurity has been developed and provided to BiH security institutions. The main purpose of the questionnaire was to assess BiH institutions' cybersecurity awareness and capabilities, focusing on topics such as cybercrime, international standards, and domestic legislation. A glossary (see annex B) reporting definitions of terms such as "cybersecurity" and "cybercrime" was appended to the questionnaire; those definitions are the ones used in this report as well. 19 institutions (see annex C) have participated in the research and answered the questionnaire. A dataset was generated to better code the answers and facilitate the analysis.

The main limitations of this study derive from the methodology adopted. Because few academic studies in English addressing BiH's cybersecurity have been produced, the desk research has been mainly centred on the collection and analysis of secondary sources from BiH public institutions and international organisations. However, some internal sources such as the cybersecurity strategy of the Ministry of Defence (MoD) are not publicly available and have not been translated into English. In addition, the author does not speak Bosnian. Hence, access to academic papers and media outlets in Bosnian was constrained.

To mitigate these limitations, the author opted for developing a questionnaire assessing the cybersecurity awareness of BiH public institutions, asking also questions concerning the existence of internal documents. Moreover, the researcher has been supported in the translation of core documents such as the 2011 *Strategy for Establishment of CERT (Computer Emergency Response Team) in Bosnia and Herzegovina* by colleagues at CSS. Nonetheless, some institutions did not answer the questionnaire. Particularly, the Herzegovina-Neretva Canton Ministry of Interior (MoI) did not participate in the research due to the stated lack of personnel and knowledge concerning cybersecurity. The Federal Ministry of Interior communicated that its answers are the ones provided by the Federal Police Administration, thus not actively providing information about the Federal MoI.

This study is intended for policymakers, academics, and citizens interested in the state of the art of cybersecurity in BiH. Particularly, this paper is designed to help BiH policymakers develop a clear assessment of the cyber capabilities of the country and its sub-state levels, identify key gaps that need to be filled and adopt policies aimed at building a cybersecurity framework and architecture in accordance with international standards and good practices. Moreover, this research has societal and research implications. Specifically, the study aims to increase the public's awareness of topics and issues related to cybersecurity and help develop a more resilient and informed society.

In addition, it aims to fulfil the research gap concerning cybersecurity in BiH by providing academics with a thorough analysis of the state of the art of cybersecurity in the country and advancing academic knowledge on the matter.

The importance of cybersecurity for Bosnia and Herzegovina

Cybersecurity has become a critical domain in international relations, and, especially, in the field of international security.[4] International and domestic economy, democratic processes, military and law enforcement are just some of the areas that have been heavily impacted by the development of technologies and cyber capabilities.[5] In BiH the importance of cybersecurity stems from three main needs: 1) ensuring the cybersecurity of critical infrastructures (CIs), private companies and citizens; 2) boosting economic growth; and 3) accomplishing international commitments and standards.

Cybersecurity encompasses a wide range of factors and issues which interest different sectors of society in BiH. BiH public sector has highlighted the necessity to implement adequate cybersecurity standards to ensure national security. Indeed, the 2015 *Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism 2015-2020* emphasises the importance of the protection of cyber CIs.[6] Ensuring the cybersecurity of critical assets has become of utmost importance for BiH due to the recent cyber-attacks affecting Western Balkan countries (e.g., North Macedonia, Serbia and Croatia).[7] Moreover, public authorities have recently been concerned with investigating cyber-attacks against media portals, namely *Žurnal* and *Buka*.[8] Nonetheless, governmental bodies are not the sole actors concerned with cybersecurity issues. Indeed, the industrial sector is particularly sensitive to cyber threats and risks. Private companies in BiH are aware of the potential detrimental aspects of digitalisation due to the negative impacts of recent phishing scams and ransomware campaigns on their business.[9] Finally, the cyber safety and rights of citizens need to be ensured. As of this, the *Civil Society & Think Tank forum* – an essential part of the Berlin Process[10] – has been calling on Western Balkan countries to engage in the digitalisation of public institutions and the protection of privacy and sensitive data.[11]

[4] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR)Relevant Theory?," *International Political Science Review* 27, no. 3 (July 2006): 221–44, https://doi.org/10.1177/0192512106064462; Nazli Choucri, *Cyberpolitics in International Relations* (Mit Press, 2012).

[5] Ibid.

[6] Bosnia and Herzegovina Council of Ministers, "Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism 2015-2020" (Bosnia and Herzegovina Council of Ministers, 2015), http://msb.gov.ba/PDF/STRATEGIJA_ZA_BORBU_PROTIV_TERORIZMA_ENG.pdf.

[7] Milica Stojanovic et al., "Cyber-Attacks a Growing Threat to Unprepared Balkan States," Balkan Insight, March 10, 2021, https://balkaninsight.com/2021/03/10/cyber-attacks-a-growing-threat-to-unprepared-balkan-states/; Matteo Mastracci, "Wave of Cyber Crimes, Political Clashes, Buffets Region," Balkan Insight, February 18, 2022, https://balkaninsight.com/2022/02/18/wave-of-cyber-crimes-political-clashes-buffets-region/.

[8] Organisation for Security and Co-operation in Europe (OSCE), "Cyber-Attacks on Online Media Endanger Media Freedom in BiH," www.osce.org, 2021, https://www.osce.org/mission-to-bosnia-and-herzegovina/479621.

[9] Eva Nagyfejeo and Sarah Puello Alfonso, "Cybersecurity Capacity Review Bosnia and Herzegovina," *SSRN Electronic Journal*, 2019, 1–87, https://doi.org/10.2139/ssrn.3658404.

[10] The Berlin Process is a platform for cooperation between representatives of the Western Balkan Six (WB6), which includes Bosnia and Herzegovina, and the Berlin Process host countries. It involves European Union institutions as well as international financial institutions. For more information, see: https://www.berlinprocess.de/.

[11] Civil Society & Think Tank Forum, "Policy Recommendations," 2021, https://wb-csf.eu/docs/Final-Recommendations-CSF2021.pdf.

In 2020, Internet users constituted 73.21% of the total population in BiH;[12] their rights and cybersecurity need to be ensured. Particularly, international organisations have warned against the threat of individuals' exposure to terrorist and extremist online propaganda.[13] This is not a minor detail as recent studies have revealed the online activism of Salafi influencers in the BiH's online sphere.[14]

Furthermore, the cyberspace can provide BiH with opportunities for economic growth.[15] Information and communication technologies (ICTs) can boost economic growth, but, at the same time, are targets of cyber criminals, thus constituting a potential economic risk public and private entities must consider.[16] This reality applies to BiH's cyberspace as well. International organisations cooperating with the government of BiH retain digital economy as a fundamental factor to boost the country's economic growth. For instance, since 2020 the United Nations Development Programme (UNDP)'s Rapid Financing Facility (RFF) donated $560,183 for the *DigitalBIZ* project which aims to steer BiH's companies towards the digital economy.[17] In addition, the United States Agency for International Development (USAID) has developed a plan which aims to support BiH's private sector in the fields of ICTs and cybersecurity, considered to be pivotal factors for BiH's economic growth.[18] Finally, the Communication Regulatory Agency (CRA) of BiH has drawn attention to the potential economic benefits deriving from the access to broadband.[19]

Nonetheless, economic advantages deriving from cyberspace can be hindered and potentially outweighed by malicious activities targeting ICTs. Tables 1, 2 and 3 illustrate the number of criminal cyberattacks recorded in the period 2019-2021 by police agencies at the state and sub-state levels. The tables also show the main trends in cybercrime identified by law enforcement; economic and financial crimes such as fraud, scams, phishing, and ransomware are the most mentioned trends. At the state level, the Directorate for Coordination of Police Bodies of BiH recorded the highest number of cybercriminal cases, amounting to a total of 554 for the period 2019-2021.

[12] World Bank, "Individuals Using the Internet (% of Population) - Bosnia and Herzegovina | Data," data.worldbank.org, accessed February 28, 2022, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BA.

[13] Organisation for Security and Co-operation in Europe (OSCE), "The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Focus on South-Eastern Europe" (Organization for Security and Co-operation in Europe (OSCE), 2018), https://polis.osce.org/role-civil-society-preventing-and-countering-violent-extremism-and-radicalization-lead-terrorism.

[14] Asya Metodieva, "The Radical Milieu and Radical Influencers of Bosnian Foreign Fighters," *Studies in Conflict & Terrorism*, January 18, 2021, 1–21, https://doi.org/10.1080/1057610x.2020.1868097.

[15] Sabina Baraković and Jasmina Baraković Husić, "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina," *Information & Security: An International Journal* 32 (2015): 131–54, https://doi.org/10.11610/isij.3205.

[16] Ioana Vasiu and Lucian Vasiu, "Cybersecurity as an Essential Sustainable Economic Development Factor," *European Journal of Sustainable Development* 7, no. 4 (October 1, 2018): 171–78, https://doi.org/10.14207/ejsd.2018.v7n4p171.

[17] United Nations Development Programme (UNDP) in Bosnia and Herzegovina, "Digital Transformation in Business – DigitalBIZ | UNDP in Bosnia and Herzegovina," United Nations Development Programme (UNDP) in Bosnia and Herzegovina, 2020, https://www.ba.undp.org/content/bosnia_and_herzegovina/en/home/development-impact/DigitalBiz.html; United Nations Development Programme (UNDP), "Digital Transformation in Business," Undp.org, 2022, https://open.undp.org/projects/00126505.

[18] The United States Agency for International Development (USAID), "Bosnia and Herzegovina. Country Development Cooperation Strategy (CDCS), December 2020 - December 2025" (The United States Agency for International Development (USAID), 2020), https://www.usaid.gov/sites/default/files/documents/BiH_CDCS_external_Dec_2025.pdf.

[19] Communications Regulatory Agency of Bosnia and Herzegovina (CRA), "Annual Report of the Communications Regulatory Agency for 2020" (Communications Regulatory Agency of Bosnia and Herzegovina (CRA), 2020), https://docs.rak.ba//documents/f8910d22-e538-4b11-9b21-4f7cfd0e0b88.pdf.

At the sub-state level, the highest number of criminal cyberattacks was registered by the Federal Police Administration and the Ministry of Internal Affairs of RS, which respectively reported a total of 354 and 452 cyberattacks in the period 2019-2021. Among the Cantons within the Federation of Bosnia and Herzegovina (FBiH), the Central Bosnia Canton, Zenica-Doboj Canton and the Tuzla Canton experienced the highest number of criminal cyberattacks, reporting respectively a total of 80, 162 and 174 cases in the period 2019-2021. 13 out of the 14 institutions providing statistics on cybercrime mentioned economic and financial cyberattacks such as frauds, ransomware and cyber industrial espionage as prominent aspects and trends of cybercrime. The Ministry of Internal Affairs of the Republic of Srpska (RS) did not mention specific facets of cybercrime but stated that there has been an increase in cybercriminal activity in the period 2019-2021. These data further testify the importance of cybersecurity for BiH, stemming from the necessity to protect its cyber infrastructures and core services in the economic and financial sphere for public institutions, private companies, and citizens.

Institution (BiH)	***N. cases 2019***	***N. cases 2020***	***N. cases 2021***	***Trends in cybercrime***
Border Police	/	/	/	Economic and financial
Directorate for Coordination of Police Bodies of BiH	132	190	232	Economic and financial
State Investigations and Protection Agency[20]	0	1	2	Economic and financial; hacking

Table 1. *Cybercrime statistics and trends by police agencies in BiH*

Institution (FBiH)	***N. cases 2019***	***N. cases 2020***	***N. cases 2021***	***Trends in cybercrime***
Federal Police Administration[21]	57/302	154/320	143/379	Economic and financial; hacking
MoI Bosnian-Podrinje Canton	6	11	8	Economic and financial
MoI Central Bosnian Canton	23	30	27	Economic and financial; hacking
MoI Posavina Canton	/	/	/	/
MoI Sarajevo Canton	2	0	3	Economic and financial;

[20] SIPA stated that it did not carry out specific investigations in the period 2019-2021 due to a lack of competence and jurisdiction to do so. However, it recorded misuses of ICTs in other criminal cases.

[21] The Federal Police Administration provided two types of statistics. The first data presented are the criminal cases which relate to Chapter thirty-two Criminal Offenses against Electronic Data Processing System of the FBiH Criminal Code. These data do not include the so-called cyber-enabled crime – traditional crimes facilitated by or committed using ICTs. The Federal Police Administration stated that there are no separate statistics, and that cyber-enabled crime often relates to the crime of fraud under article 294 of the FBiH Criminal Code. The second data provided by the Federal Police Administration are fraud crimes which, according to the institution, have been primarily committed through the misuse of ICTs.

				hacking
MoI Tuzla Canton	34	56	84	/
MoI Una-Sana Canton	3	3	36	Economic and financial; hacking
MoI West Herzegovina Canton	1	0	2	Economic and financial
MoI Zenica-Doboj Canton	28	54	80	Economic and financial; hacking

Table 2. *Cybercrime statistics and trends by police agencies in FBiH*

Institution (RS, BD)	***N. cases 2019***	***N. cases 2020***	***N. cases 2021***	***Trends in cybercrime***
Ministry of Internal Affairs of Republic of Srpska	117	189	146	General increase in cybercrime
Police Brčko District	4	2	7	Economic and financial

Table 3. *Cybercrime statistics and trends by police agencies in RS and BD*

Finally, international commitments and standards (Figure 1)[22] render cybersecurity a key domain for BiH. International commitments originate from BiH's participation in intergovernmental organisations like the OSCE as well as from international treaties such as the Council of Europe Convention on Cybercrime – commonly known as the Budapest Convention. The OSCE has defined as 'politically binding on Bosnia and Herzegovina' the organisation's CBMs in cyberspace developed through the *2016 Decision no. 1202*.[23] Furthermore, the Budapest Convention is a binding treaty which therefore establishes requirements to comply with.[24] Moreover, ensuring international cyber standards is fundamental as BiH aims to access the EU. This requires the adoption of the EU's legislation and policies on cybersecurity, including the General Data Protection Regulation (GDPR) and the EU Network and Information Security (NIS) Directive which are pre-requisites to enhancing the European Digital Single Market. In addition, BiH aims to become a member of NATO. Such a step requires meeting specific obligations, including the respect of cybersecurity standards.[25] Finally, other minor but key international organisations BiH is part of such as the Central European Initiative have stated the strengthening of cybersecurity among their goals, thus encouraging BiH to move towards this direction.[26]

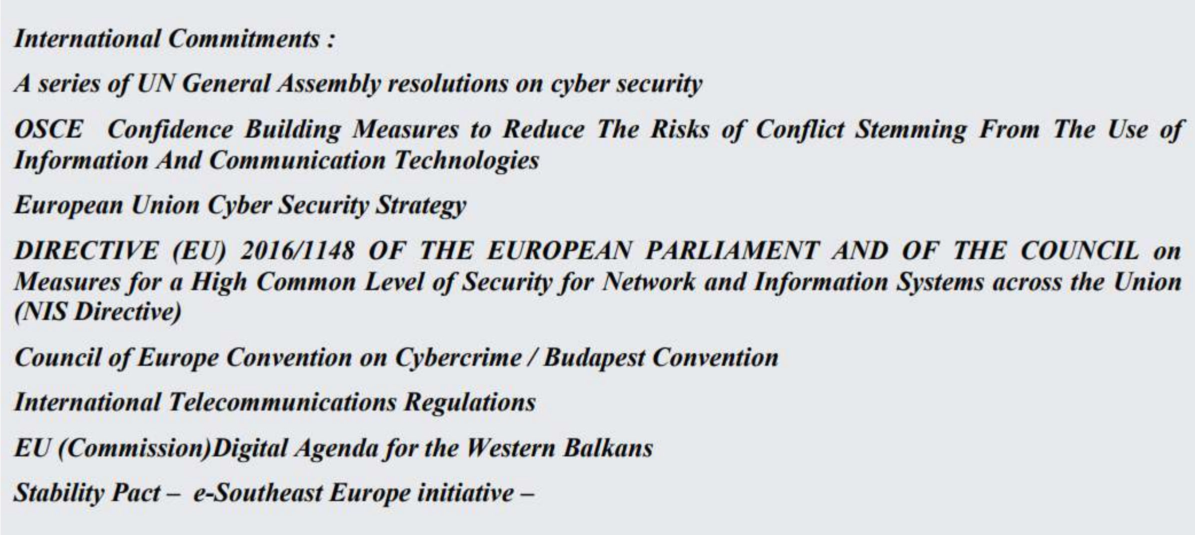
[22] Organisation for Security and Co-operation in Europe (OSCE), "Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina," *Www.osce.org* (Organisation for Security and Co-operation in Europe (OSCE), 2019), https://www.osce.org/mission-to-bosnia-and-herzegovina/438383.

[23] Ivi., 7.

[24] Jonathan Clough, "The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World," *Criminal Law Forum* 23, no. 4 (September 25, 2012): 363–91, https://doi.org/10.1007/s10609-012-9183-3.

[25] Eva Nagyfejeo and Sarah Puello Alfonso, "Cybersecurity Capacity Review Bosnia and Herzegovina," *SSRN Electronic Journal*, 2019, 1–87, https://doi.org/10.2139/ssrn.3658404.

[26] Central European Initiative (CEI), "CEI Plan of Action 2021-2023" (Central European Initiative (CEI), 2020), https://www.cei.int/sites/default/files/publications/downloads/CEI%20Plan%20of%20Action%20DIGITAL%20ESEC%20FINAL.pdf.



International Commitments :

A series of UN General Assembly resolutions on cyber security

OSCE Confidence Building Measures to Reduce The Risks of Conflict Stemming From The Use of Information And Communication Technologies

European Union Cyber Security Strategy

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Security for Network and Information Systems across the Union (NIS Directive)

Council of Europe Convention on Cybercrime / Budapest Convention

International Telecommunications Regulations

EU (Commission)Digital Agenda for the Western Balkans

Stability Pact – e-Southeast Europe initiative –

Figure 1. *Summary of international commitments of BiH in the field of cybersecurity*

BiH's jeopardised but improving approach to cybersecurity

BiH's approach to cybersecurity has been labelled as jeopardised.[27] BiH's complex system of governance brings about an unharmonized legislation on cybersecurity which is enacted by different public bodies at different governmental levels.[28] Although BiH has taken important steps to produce core laws and regulations on cybersecurity, the country lacks a well-defined national cybersecurity strategy which can pave the way for the development of further legislation and policies. Despite this, BiH has been supporting international efforts to regulate the cyberspace, thus being actively involved in international fora.

The three sub-state entities constituting BiH – the Federation of Bosnia and Herzegovina (FBiH), the Republic of Srpska (RS) and the Brčko District (BD) – tackle cybersecurity issues through different laws.[29] Indeed, these entities present their own Criminal Codes and Criminal Procedural Codes that address cybercrime, thus dispersing cyber-related issues under different laws. Moreover, these laws are enacted by different bodies at different levels without clear and efficient coordination.[30] The different laws produced constitute the legislative body addressing the issues of cybersecurity and cybercrime at both the state and sub-state levels (Figures 2 and 3).[31]

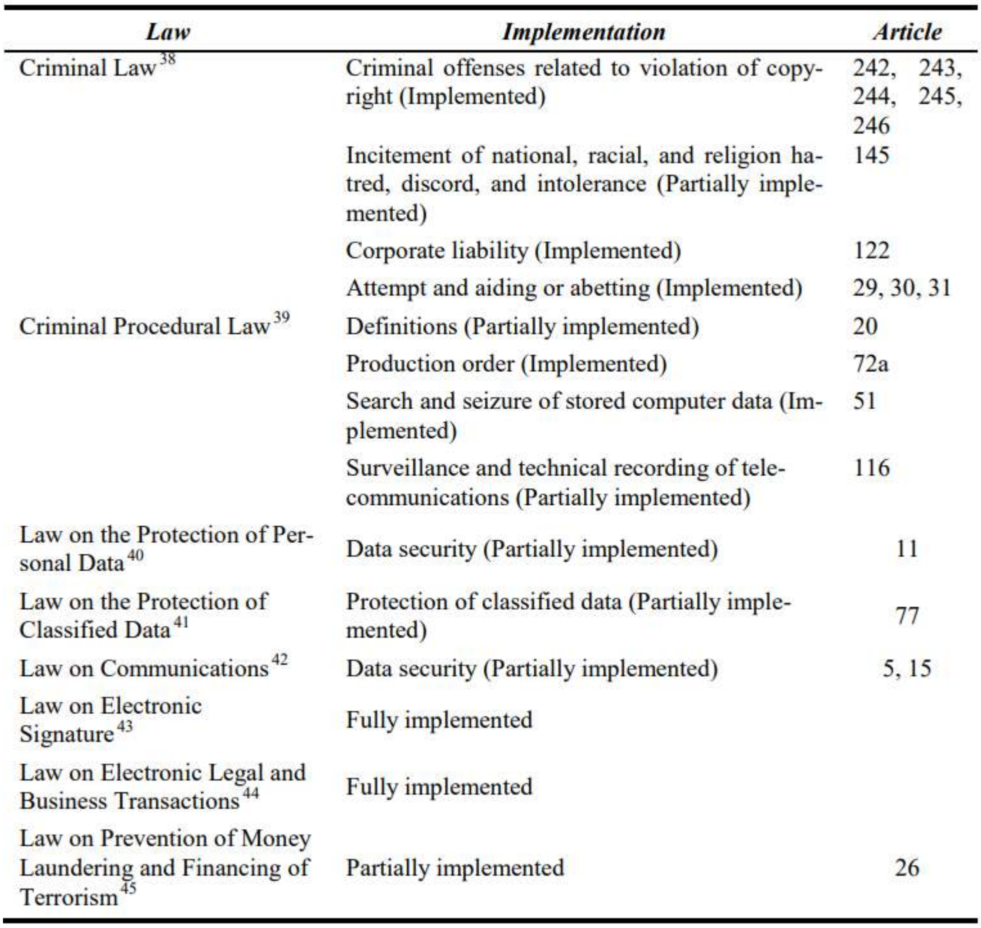
[27] Sabina Baraković and Jasmina Baraković Husić, "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina," *Information & Security: An International Journal* 32 (2015): 131–54, https://doi.org/10.11610/isij.3205.

[28] Zvezdan Stojanović and Mehrudina Musić, "Development of E-Government in Bosnia and Herzegovina," *Journal Human Research in Rehabilitation* 8, no. 1 (April 2018): 70–76, https://doi.org/10.21554/hrr.041810.

[29] Sabina Baraković and Jasmina Baraković Husić, "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina," *Information & Security: An International Journal* 32 (2015): 131–54, https://doi.org/10.11610/isij.3205.

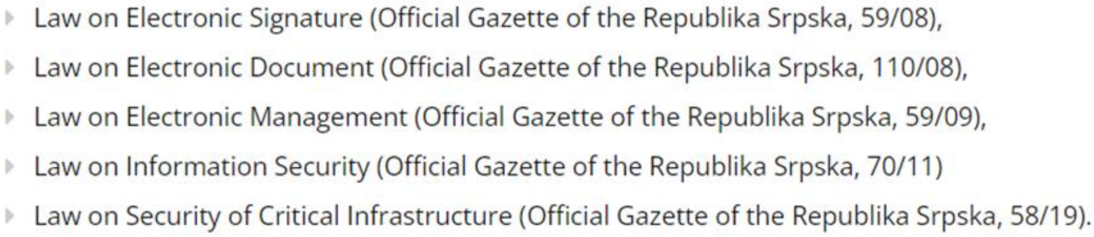
[30] Eva Nagyfejeo and Sarah Puello Alfonso, "Cybersecurity Capacity Review Bosnia and Herzegovina," *SSRN Electronic Journal*, 2019, 1–87, https://doi.org/10.2139/ssrn.3658404.

[31] Council of Europe, "Bosnia and Herzegovina. Octopus Cybercrime Community," 2017, https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/AZnxfNT8Y3Zl/content/bosnia-and-



Law	*Implementation*	*Article*
Criminal Law[38]	Criminal offenses related to violation of copyright (Implemented)	242, 243, 244, 245, 246
	Incitement of national, racial, and religion hatred, discord, and intolerance (Partially implemented)	145
	Corporate liability (Implemented)	122
	Attempt and aiding or abetting (Implemented)	29, 30, 31
Criminal Procedural Law[39]	Definitions (Partially implemented)	20
	Production order (Implemented)	72a
	Search and seizure of stored computer data (Implemented)	51
	Surveillance and technical recording of telecommunications (Partially implemented)	116
Law on the Protection of Personal Data[40]	Data security (Partially implemented)	11
Law on the Protection of Classified Data[41]	Protection of classified data (Partially implemented)	77
Law on Communications[42]	Data security (Partially implemented)	5, 15
Law on Electronic Signature[43]	Fully implemented	
Law on Electronic Legal and Business Transactions[44]	Fully implemented	
Law on Prevention of Money Laundering and Financing of Terrorism[45]	Partially implemented	26

Figure 2. *State level legislation related to cybersecurity*



- Law on Electronic Signature (Official Gazette of the Republika Srpska, 59/08),
- Law on Electronic Document (Official Gazette of the Republika Srpska, 110/08),
- Law on Electronic Management (Official Gazette of the Republika Srpska, 59/09),
- Law on Information Security (Official Gazette of the Republika Srpska, 70/11)
- Law on Security of Critical Infrastructure (Official Gazette of the Republika Srpska, 58/19).

Figure 3. *Sub-state regulations related to cybersecurity*

Although the above-mentioned legislation testifies BiH's efforts in the field of cybersecurity, as of 2022, BiH does not present a national cybersecurity strategy (NCSS) and few national strategic documents address cybersecurity issues. Among others, the 2011 *Strategy for Establishing CERT in Bosnia and Herzegovina* constitutes a fundamental step in the field of cybersecurity as it shows a certain degree of cyber awareness, defining the lack of adequate cyber capabilities and infrastructures as a vulnerability and threat to the country and acknowledging the importance of

herzegovina?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_AZnxfNT8Y3Zl%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_pos%3D1%26p_p_col_count%3D2?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2; Organisation for Security and Co-operation in Europe (OSCE), "Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina," *Www.osce.org* (Organisation for Security and Co-operation in Europe (OSCE), 2019), https://www.osce.org/mission-to-bosnia-and-herzegovina/438383.

cybersecurity to meet international, especially European, standards.[32] In addition, the 2015 *Strategy of Bosnia and Herzegovina for preventing and combating terrorism 2015-2020* is a core document that deems the establishment of *Computer Emergency Response Team* (CERT) as 'essential' to protect cyber CIs.[33] However, despite this document and the precedent 2011 strategy for the establishment of CERT such a body has not been created yet.[34] The 2015 strategy further emphasises the importance of building biometric data collection capabilities as well as the enhancement of international cooperation to monitor and tackle the terrorist use of ICTs.[35] Finally, the 2017 *Strategy for Fight against Organised Crime in Bosnia and Herzegovina (2017-2020)* constitutes another pivotal strategic paper concerning cybersecurity as it mentions cybercrime,[36] thus paying attention to a crucial threat in the cyberspace. However, as previously stated, these documents do not provide a systemic approach to cybersecurity and, especially with concern to the 2011 strategy, their core objectives remain unaccomplished.

Despite these issues in the approach adopted, BiH has taken important domestic and international actions in some cyber-related areas. For instance, attention has been dedicated to ensuring the cyber safety and security of citizens. Particularly, data protection and privacy are ensured by the *Personal Data Protection Agency* in BiH which implements the *Law on Protection of Personal Data*.[37] The agency aims also to ensure standards which align with the EU's GDPR.[38] Moreover, BiH is working to protect the online personal safety of children who are at risk of suffering from online abuse; in 2014 the *Council of Ministers* developed an action plan dedicated to the online protection of children.[39] Furthermore, some institutions adopted internal documents concerning cybersecurity. For instance, the High Judicial and Prosecutorial Council of BiH adopted the *Security Policy of the Judicial Information System of Bosnia and Herzegovina* in 2016, defining binding internal standards, rules and procedures to ensure the security of its ICTs.[40]

[32] Ministry of Security of Bosnia and Herzegovina, "Strategy for Establishing CERT in Bosnia and Herzegovina" (Ministry of Security of Bosnia and Herzegovina, 2011), http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA.

[33] Bosnia and Herzegovina Council of Ministers, "Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism 2015-2020" (Bosnia and Herzeoginva Council of Ministers, 2015), http://msb.gov.ba/PDF/STRATEGIJA_ZA_BORBU_PROTIV_TERORIZMA_ENG.pdf, 10.

[34] Organisation for Security and Co-operation in Europe (OSCE), "Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina," *Www.osce.org* (Organisation for Security and Co-operation in Europe (OSCE), 2019), https://www.osce.org/mission-to-bosnia-and-herzegovina/438383.

[35] Bosnia and Herzegovina Council of Ministers, "Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism 2015-2020" (Bosnia and Herzeoginva Council of Ministers, 2015), http://msb.gov.ba/PDF/STRATEGIJA_ZA_BORBU_PROTIV_TERORIZMA_ENG.pdf, 10.

[36] Bosnia and Herzegovina Council of Ministers, "Strategy for Fight against Organised Crime in Bosnia and Herzegovina (2017-2020)," 2017, http://www.msb.gov.ba/PDF/strategy11122017.pdf.

[37] Personal Data Protection Agency in Bosnia and Herzegovina, "Competencies," www.azlp.ba, accessed February 25, 2022, http://www.azlp.ba/o_agenciji/nadleznosti/default.aspx?id=459&langTag=en-US&template_id=149&pageIndex=1.

[38] Personal Data Protection Agency in Bosnia and Herzegovina, "Regulation (EU) 2016/679 of the European Parliament and of the Council," azlp.ba, accessed February 25, 2022, http://azlp.ba/GDPR_Menu/Opsta_uredba/default.aspx?id=2366&langTag=en-US&template_id=149&pageIndex=1.

[39] Bosnia and Herzegovina Council of Ministers, "Action Plan for Child Protection and Prevention of Violence against Children through Information-Communications Technologies in Bosnia and Herzegovina 2014-2015," 2014, http://msb.gov.ba/PDF/140605_Nasilje_engleski_SG_ver2.pdf.

[40] High Judicial and Prosecutorial Council of Bosnia and Herzegovina, "Politika Sigurnosti Pravosudnog Informacionog Sistema Bosne I Hercegovine [Security Policy of the Judicial Information System of Bosnia and Herzegovina]" (High Judicial and Prosecutorial Council of Bosnia and Herzegovina, 2016), https://portalfo1.pravosudje.ba/vstvfo-api/vijest/download/44943.

Moreover, the answers provided to the questionnaire have revealed the existence of other documents such as the 2017 cyber strategy of the Ministry of Defence – which, however, is not available online – mentioned by both MoD and other institutions such as SIPA.

Finally, from an international perspective, BiH participates in pivotal intergovernmental organisations in the field of cybersecurity such as the International Telecommunication Union,[41] the United Nations' (UN) specialized agency for information and communication technologies. Moreover, BiH has signed and ratified the *Budapest Convention on Cybercrime*, considered the most comprehensive international treaty addressing cybercrime.[42] Furthermore, as previously stated, BiH is part of OSCE which, through its mission to BiH, is engaging in cooperation and capacity building with BiH institutions. This aspect will thoroughly be discussed later in the report.

BiH's cybersecurity gaps and improvements and their implications

Although BiH has developed some core measures and legislation to advance in the field of cybersecurity, there are still key gaps to fill. In 2019, the *Global Cyber Security Capacity Centre* (GCSCC) has evaluated the country's cybersecurity capabilities and ranked them accordingly.[43] Particularly, GCSCC has analysed 5 dimensions of BiH's cyber capabilities: 1) **cybersecurity policy and strategy**; 2) **cybersecurity culture and society**; 3) **cybersecurity training, education, and skills**; 4) **legal and regulatory frameworks**; and 5) **standards, organisations and technologies**.

In the first dimension, BiH is at an early stage. No national cyber strategy exists, but consultations between ministries and between governmental bodies and international partners are ongoing. Furthermore, no CERT is in place, there is not a central registry for cyber incidents and there are no mandatory reporting requirements for cyber incidents. Moreover, there is no clear categorisation and monitoring of CIs, especially in the field of cybersecurity, and an almost absolute lack of cyber crisis management (e.g., risk management exercises, and cyber drills).

In the second dimension, BiH is at an initial stage. Both public and private sectors present a low level of cyber awareness and limited knowledge of cyber threats and risks. Moreover, law enforcement has been the primary reporting mechanism on cybercrime with a lack of national coordination between the different police departments and units operating in the sub-state entities. Similarly, **in the third dimension**, BiH presents low cyber capabilities with generally poor and underdeveloped cyber courses and trainings at the primary, secondary and bachelor's educational levels. Cyber-tailored courses only exist at the higher university level (e.g., masters, and PhDs).

In the fourth dimension, BiH has made some improvements. Especially, despite being jeopardised and dispersed under different sub-state entities' legislation, the country's legal system addresses

[41] International Telecommunication Union (ITU), "Bosnia and Herzegovina," www.itu.int, accessed February 28, 2022, https://www.itu.int/online/mm/scripts/gensel9?_ctryid=1000100548.

[42] International Criminal Police Organisation (INTERPOL), "National Cybercrime Strategy Guidebook" (International Criminal Police Organisation (INTERPOL), 2021), file:///C:/Users/HP/Downloads/National%20Cybercrime%20Strategy%20Guidebook%20(1).pdf.

[43] Eva Nagyfejeo and Sarah Puello Alfonso, "Cybersecurity Capacity Review Bosnia and Herzegovina," *SSRN Electronic Journal*, 2019, 1–87, https://doi.org/10.2139/ssrn.3658404.

cyber-related issues, including cybercrime. However, in the judicial system, there is no specialised unit combating cybercrime and the fight against it remains un-coordinated and responsibility of different bodies. Lastly, **in the fifth dimension**, BiH has made progress, but more actions are needed. Although there are laws concerning standardisation and alignment with international good practices, there is a lack of awareness concerning cybersecurity international standards. Finally, BiH's domestic market does not offer cybersecurity products, thus relying mainly on international producers.

The observations made by GCSCC are shared by researchers and international organisations attentive to the state of the art of cybersecurity in BiH. Scholars have emphasised the necessity to harmonise legislation, develop a national cybersecurity strategy, establish specialised cybersecurity units within the ministers and create a national CERT.[44] Furthermore, exposure to emerging cyber threats such as the terrorist and criminal use of cryptocurrencies can bring about economic problems for BiH.[45] Moreover, the absence of a national CERT has been emphasised by the OSCE. Despite being considered essential by the 2015 *Strategy of Bosnia and Herzegovina for preventing and combating terrorism 2015-2020*, a national CERT has not been developed yet and BiH remains 'the only country in South-Eastern Europe without a national level cybersecurity strategy and CERT.'[46] Within BiH, CERT is operational only in the Republic of Srpska since 2015 and works under the *Ministry for Scientific and Technological Development, Higher Education, and Information Society* since 2019.[47] Finally, in 2021 the EU produced a key report assessing BiH's steps towards the integration with the EU, emphasising the necessity for higher cybersecurity standards as a requirement for access.[48] Among other issues, the report dedicates particular attention to the need to implement the Budapest Convention and develop efficient anti-cybercrime capabilities.[49]

Cybersecurity improvements and gaps as of 2022

Although in 2019 BiH presented evident cybersecurity gaps that persist to a certain extent, the desk research and analysis and the questionnaire's results suggest some positive shifts and improvements.

Cybersecurity is being considered a priority by 13 out of the 19 institutions that participated in the research. However, only 10 out of 19 institutions state they have internal documents concerning cybersecurity. For instance, SIPA mentioned a 'rulebook on protection of security of SIPA information and communication system' and 'instruction on the use of the Internet in SIPA.'

[44] Sabina Baraković and Jasmina Baraković Husić, "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina," *Information & Security: An International Journal* 32 (2015): 131–54, https://doi.org/10.11610/isij.3205.

[45] Nikolina Maleta and Ivana Stipanovic, "Difficulties in Procedure of Obtaining Evidence on Money Laundering through Cryptocurrencies as a Possible Threat to the Market Stability," in *Economic and Social Development (Book of Proceedings), 31st International Scientific Conference on Economic and Social Development - "Legal Challenges of Modern World,"* ed. Marijan Cingula, Douglas Rhein, and Mustapha Machrafi, 2018, https://is.muni.cz/repo/1420998/Book_of_Proceedings_esdSplit2018_Online.pdf#page=598.

[46] Organisation for Security and Co-operation in Europe (OSCE), "Cyber Security" (Organisation for Security and Co-operation in Europe (OSCE)), accessed February 25, 2022, https://www.osce.org/files/f/documents/c/4/468369.pdf, 1.

[47] CERT Republic of Srpska, "Republic of Srpska National CERT | About," CERTRS.org, July 8, 2019, https://certrs.org/en/about/.

[48] European Commission, "Bosnia and Herzegovina 2021 Report," 2021, file:///C:/Users/HP/Downloads/Bosnia%20and%20Herzegovina%202021%20report.PDF.

[49] Ibid.

Similarly, the Agency for Police Support, operating under the Ministry of Security, stated to have some internal regulations addressing the protection of ICTs. Moreover, few institutions are aware of relevant state level documents concerning cybersecurity. 12 out of 19 institutions stated to be able to mention relevant state documents concerning cybersecurity. Tables 4, 5, and 6 show the institutions' knowledge and awareness of state level documents and report the documents cited by them. All of the institutions at the state level are aware of state level documents and were able to mention some, while at the sub-state level the questionnaire has revealed a concerning lack of knowledge, especially among FBiH's cantons. Within FBiH, the Federal Police Administration and the Judicial Police are the institutions the most aware and knowledgeable about cybersecurity documents. Conversely, only 2 out of the 8 Cantons that answered the questionnaire were able to cite some documents. In RS, the Ministry of Internal Affairs was not able to mention any state level document, while the Police of BD cited two core documents.

Interestingly, the *Guidelines for a strategic Cybersecurity Framework in BiH* – which was drafted by OSCE and will be discussed in the next chapters of this report – was the most mentioned state level document together with the Budapest Convention. Other state level documents mentioned were the 2011 *Strategy for Establishment of CERT (Computer Emergency Response Team) in Bosnia and Herzegovina*, the *Information Society Development Policy of Bosnia and Herzegovina for the period 2017-2021* and the *cybersecurity strategy of the MoD*. Other documents mentioned as 'state level documents' are, in fact, sub-state legislation such as the *criminal and procedural Codes of FBiH and RS.*

Institution (BiH)	*Knowledge*	*Documents mentioned*
AEPTM	Yes	Guidelines for a strategic Cybersecurity Framework in BiH
AFIV	Yes	The Criminal Code of FBiH and the Criminal Procedure Code of RS
Agency for Police Support	Yes	Guidelines for a strategic Cybersecurity Framework in BiH
Border Police	Yes	Guidelines for a strategic Cybersecurity Framework in BiH
DCPB	Yes	Guidelines for a strategic Cybersecurity Framework in BiH, Decision on Information Security Management in BiH Institutions, Information Society Development Policy of Bosnia and Herzegovina for the period 2017-2021
MoD	Yes	Guidelines for a strategic Cybersecurity Framework in BiH; information security management policy for the period 2017-2022 for BiH institutions; 2017 decision of the Council of Ministers of BiH on the establishment of CERT for the institutions of BiH
SIPA	Yes	Cybercrime Convention; Additional Protocol to the Convention on Cybercrime; Cyber Security Strategy - establishment of a system for ensuring a high level of cybersecurity in the MoD and the Armed Forces of

		BiH; CERT establishment strategy in BiH

Table 4. *Knowledge of state level documents and state level documents cited by BiH institutions*

Institution (FBiH)	*Knowledge*	*Documents mentioned*
Federal Police Administration	Yes	Guidelines for a strategic Cybersecurity Framework in BiH
Judicial Police	Yes	Security Policy of the BiH Judicial Information System
MoI Bosnian-Podrinje Canton	No	/
MoI Central Bosnian Canton	Yes	Decision to ratify the Convention on Cybercrime
MoI Posavina Canton	No	/
MoI Sarajevo Canton	No	/
MoI Tuzla Canton	No	/
MoI Una-Sana Canton	Yes	Criminal Code of FBiH and the Law, Criminal Code of RS
MoI West Herzegovina Canton	No	/
MoI Zenica-Doboj Canton	No	/

Table 5. *Knowledge of state level documents and state level documents cited by FBiH institutions*

Institution (RS, BD)	*Knowledge*	*Documents mentioned*
Ministry of Internal Affairs of RS	/	/
Police BD	Yes	Guidelines for a strategic Cybersecurity Framework in BiH; Strategy for the establishment of CERT

Table 6. *Knowledge of state level documents and state level documents cited by RS and BD institutions*

Despite these gaps, there is an increased cyber awareness concerning both the threats and risks of cyberspace and international standards and good practices. Indeed, only 4 out of 19 institutions – namely AFIV, AEPTM, the Judicial Police of FBiH and the MoI of the Posavina Canton – had not participated in cybersecurity training courses, workshops, and seminars in the 2019-2022 period. Moreover, as previously shown in tables 1, 2, and 3, institutions were able to provide cybercrime statistics and mention trends in cybercrime, addressing diverse factors connected to it.

Besides economic and financial cybercrime, institutions have mentioned other trends characterising cybercrime. Specifically, AEPTM cited numerous aspects of cybercrime including online hate speech, child sexual abuse material and illicit trafficking in arms, organs, and drugs.

Furthermore, 12 out of 19 institutions mentioned international standards and good practices BiH should align with. Among others, the *ISO 27000* family of standards was the most cited, but other international practices such as the *Budapest Convention* and *EU laws* (e.g., NIS directive, and GDPR) were mentioned as examples as well. Other cybersecurity standards cited were the *Payment Card Industry Data Security Standard* (PCI DSS), the *ISO/IEC 15408 and 17799 standards*, the *Financial Industry Regulatory Authority's standards*, and the *US Department of Health and Human Services' cybersecurity requirements and procedures*. Tables 7, 8 and 9 show the awareness of international standards and good practices at the state and sub-state levels. While institutions at the state level are more aware and knowledgeable about cybersecurity standards, the sub-state level suffers from evident gaps. Within FBiH, 6 out of 10 institutions were not able to mention international standards. Neither could the Ministry of Internal Affairs of RS mention any international standards.

Institution (BiH)	***Knowledge***	***Documents mentioned***
AEPTM	Yes	ISO 17799, ISO 15408
AFIV	Yes	ISO 27001; PCI DSS - Payment Card Industry Data Security Standard
Agency for Police Support	Yes	ISO/IEC 27001 and 27002
Border Police	Yes	ISO/IEC 27001, PCI DSS, HIPAA, FINRA, GDPR
DCPB	Yes	Budapest Convention
MoD	Yes	NIS Directive (EU) 2016/1148; General Data Protection Directive (EU Directive 2016/679); Stability Pact - eSoutheast Europe Initiative - eSEE 2007; Budapest Convention
SIPA	Yes	Cybercrime Convention; ENISA Directive; NIS directive; Regulation (EU) 2016/279 of the European Parliament and of the Council of 27 April 2016 years, etc.

Table 7. *Knowledge of international standards and good practices and documents cited by BiH institutions*

Institution (FBiH)	***Knowledge***	***Documents mentioned***
Federal Police Administration	Yes	ISO 27001; GDPR; standards related to the financial sector (banks, payment cards, etc.)
Judicial Police	No	/
MoI Bosnian-Podrinje Canton	No	/
MoI Central Bosnian Canton	No	/
MoI Posavina Canton	No	/
MoI Sarajevo	No	/

Canton		
MoI Tuzla Canton	No	/
MoI Una-Sana Canton	Yes	European Convention on Cybercrime
MoI West Herzegovina Canton	Yes	ISO2701; FINRA; GDR
MoI Zenica-Doboj Canton	Yes	Budapest Convention

Table 8. *Knowledge of international standards and good practices and documents cited by FBiH institutions*

Institution (RS, BD)	***Knowledge***	***Documents mentioned***
Ministry of Internal Affairs of RS	No	/
Police BD	Yes	ISO/IEC 27032:2015

Table 9. *Knowledge of international standards and good practices and documents cited by RS and BD institutions*

Finally, the institutions' self-assessment of cyber capabilities has revealed some interesting facts and figures. Tables 10, 11, and 12 illustrate the results of the self-assessment. According to the institutions, only the MoI of the Central Bosnian Canton was a victim of cyberattack(s) in the period 2019-2022. Concerningly, the MoI of the Sarajevo Canton stated that it does not have information to answer whether the institution was or was not a victim of cyberattack(s) in 2019-2022, to assess its cyber capabilities and to evaluate citizens' cyber awareness. Institutions at the state level argue they present enhanced cyber capabilities, while this self-assessment diverges at the sub-state level. Especially, cantons within FBiH declare to have capacities ranging from fair to good. Similarly, while the RS Ministry of Internal Affairs states to have good cyber capabilities, the Police of BD argues to have only fair cyber capabilities. All institutions agree on ranking citizens' cyber awareness as low, ranging from poor to average.

Institution (BiH)	***Victim of cyberattack***	***Cyber capabilities***	***Citizens' awareness***
AEPTM	No	Average	Average
AFIV	No	Average	Fair
Agency for Police Support	No	Good	Fair
Border Police	No	Good	Fair
DCPB	No	Average	Fair
MoD	Yes	Good	Fair
SIPA	No	Good	Average

Table 10. *Self-assessment of cyber capabilities by BiH institutions*

Institution (FBiH)	*Victim of cyberattack*	*Cyber capabilities*	*Citizens' awareness*
Federal Police Administration	No	Good	Average
Judicial Police in FBiH	No	Average	Fair
MoI Bosnian-Podrinje Canton	No	Average	Fair
MoI Central Bosnian Canton	Yes	Fair	Fair
MoI Posavina Canton	No	Fair	Fair
MoI Sarajevo Canton	/	/	/
MoI Tuzla Canton	No	Good	Fair
MoI Una-Sana Canton	No	Fair	Fair
MoI West Herzegovina Canton	No	Fair	Poor
MoI Zenica-Doboj Canton	No	Good	Fair

Table 11. *Self-assessment of cyber capabilities by FBiH institutions*

Institution (RS, BD)	*Victim of cyberattack*	*Cyber capabilities*	*Citizens' awareness*
Ministry of Internal Affairs of RS	No	Good	Average
Police BD	No	Fair	Fair

Table 12. *Self-assessment of cyber capabilities by RS and BD institutions*

Core implications of cybersecurity gaps

These cybersecurity gaps lead to some pivotal implications for the country’s national security:

- The lack of a national cyber strategy, a national CERT and of CIs’ monitoring seriously undermines cyber risk assessment and prompt response to cyber incidents, thus exposing key national assets to risks and threats.
- The low level of cyber awareness and culture in both the public and private sectors exposes governmental bodies, private companies, and citizens to cyber threats, especially cybercrime.
- The divergencies in the number of cyber courses and trainings offered to public employees undermine the development of an overall enhanced state cyber capabilities.
- The low level of coordination between police units and departments at the national and sub-national levels constitutes an obstacle to the effective and efficient fight against cybercrime.
- The low level of indigenous cyber capabilities fosters the country’s reliance on international producers.
- The underdeveloped nature of cyber capabilities in BiH can slow the process of integration with the EU and BiH’s access to NATO, thus undermining BiH’s long-standing international aspirations.

International and domestic cooperation and support to build cyber capabilities

Both desk analysis and the questionnaire have revealed the pivotal role international support plays in strengthening BiH's cyber capabilities. The support of partner countries, the use of international funds, and the engagement in international training programmes are core factors to boost BiH's cybersecurity capabilities.

Particularly, the questionnaire has revealed that international organisations, partner countries and research centres are playing a crucial role in supporting and building BiH public institutions' cyber capabilities. In the period 2019-2021, 15 out of 19 institutions participated in courses, workshops, and seminars on cybersecurity-related issues. Numerous of these opportunities have been offered either by international organisations and partner countries or by other actors using international funds. Tables 13, 14, and 15 show the number of courses and their providers for both the state and sub-state levels. The data show that BiH, FBiH, RS and BD institutions are benefitting from courses to different extents. Institutions in FBiH are the ones that participated in the highest number of courses. The Federal Police Administration and the RS Ministry of Internal Affairs could not provide exact figures, but they stated that they had been taking part in several courses.

Institution (BiH)	***N. courses***	***Courses providers***
AEPTM	/	/
AFIV	/	/
Agency for Police Support	7	Ministry of Security (Twinning project "EU4 Fight Against Cybercrime in BiH")
Border Police	20	US Embassy, CEPOL, Federal Police Administration and RS Ministry of the Interior, Twinning Project, Sys Company, BiH Civil Service Agency, IPA
DCPB	/	OSCE Mission to Bosnia and Herzegovina, Council of Europe, Ministry of Security of BiH within the IPA 2017 Twinning Project
MoD	13+	OSCE Mission to BiH/BiH Ministry of Defence, Ministry of Defence of BiH/Ministry of Defence of the Republic of Italy, US Adriatic Charter (A5), Ministry of Defence of BiH/NG of the State of Maryland, US, OSCE Mission to BiH/BiH Ministry of Security
SIPA	41	Embassy of the United States of America, French Embassy, CSOs; DCAF, IPA 2017, CEPOL, ICITAP, OSCE, TAIEX, EUROPOL, UNODC, High Judicial and Prosecutorial Council of Bosnia and Herzegovina, Ministry of Security of Bosnia and Herzegovina, Council of Europe, SELEC and GIZ

Table 13. *Number of cyber training courses BiH institutions participated in in the period 2019-2021 and courses' providers*

Institution (FBiH)	*N. courses*	*Courses providers*
Federal Police Administration	Several courses	OSCE, UNDP, US Embassy in Sarajevo (ICITAP, USAID), Council of Europe and European Commission through various IPA projects, French Embassy in Sarajevo, UK Embassy and others
Judicial Police in FBiH	/	/
MoI Bosnian-Podrinje Canton	10	Project EU4 Fight Against Cybercrime in BiH
MoI Central Bosnian Canton	23	OSCE BiH; Ministry of Security of BiH within the IPA project
MoI Posavina Canton	/	/
MoI Sarajevo Canton	16	Embassy of the Kingdom of Saudi Arabia, Ministry of Security of BiH, OSCE in BiH, IPA 2103, EU 4 Fight against cybercrime in BiH, IPA 2017 Twinning project
MoI Tuzla Canton	50	Ministry of Security of BiH; Federal Police Administration; OSCE; Faculty of Criminology, Criminology and Security Studies Sarajevo; Turkish Cooperation and Coordination Agency
MoI Una-Sana Canton	1	EUROPOL - eComm Action 2020 awareness campaign
MoI West Herzegovina Canton	16	FUP-e; OSCE; Ministry of Security; IPA
MoI Zenica-Doboj Canton	1	MoI information Department Zenica-Doboj Canton

Table 14. *Number of cyber training courses FBiH institutions participated in in the period 2019-2021 and courses' providers*

Institution (RS, BD)	*N. courses*	*Courses providers*
Ministry of Internal Affairs of RS	/	The George C. Marshall European Center for Security Studies; OSCE; Interpol; Europol; International projects: IPROCEEDS, IPA, etc.
Police BD	4	OSCE; CEPOL; Faculty of Criminology, Criminology and Security Studies Sarajevo

Table 15. *Number of cyber training courses RS and BD institutions participated in in the period 2019-2021 and courses' providers*

Academic centres, private sector and BiH public institutions

Both the academia and the private sector are playing a small but important role in providing training courses to BiH public institutions. 2 out of 19 institutions mentioned the Faculty of Criminalistics, Criminology and Security Studies as providers. The Ministry of Internal Affairs of the Republic of Srpska mentioned the George C. Marshall European Center for Security Studies, while SIPA mentioned the Geneva Centre for Security Sector Governance. The Border Police of BiH was the only institution that mentioned a private sector provider, the private firm *Sys Company*.

BiH public institutions are playing a more prominent role. The Ministry of Security was mentioned as a provider by 6 institutions. The Border Police of BiH was the only institution to mention the BiH Civil Service Agency and the Ministry of the Interior of RS as providers. Together with the Ministry of Interior of the Tuzla Canton, the Border Police was the only institution to cite the Federal Ministry of Internal Affairs. Finally, SIPA also mentioned the High Judicial and Prosecutorial Council of BiH as a provider.

Countries

The answers to the questionnaire show that partner countries are supporting BiH in the cybersecurity field through the work and cooperation of both Western and non-Western embassies, national agencies, and NGOs.

The Federal Police Administration and the Border Police mentioned the US embassy as a provider. The Federal Police Administration also mentioned the UK embassy and the Embassy of France. SIPA mentioned both the US and the French embassies. Furthermore, SIPA mentioned the *Deutsche Gesellschaft für Internationale Zusammenarbeit* – whose main commissioning party is Germany's Ministry for Economic Cooperation and Development –[50] and the International Criminal Investigative Training Assistance Program – which is situated in the US Department of Justice's Criminal Division.[51] Finally, the Federal Police Administration also mentioned USAID as a provider of training courses on cybersecurity and the Ministry of Defence mentioned the MoD of the Republic of Italy.

Non-western countries are providing support as well. China is offering cooperation through the work of Huawei company which is present in the country and has held meetings with BiH high-ranking officials.[52] In addition, the Ministry of Interior of the Sarajevo Canton mentioned the embassy of Saudi Arabia as a provider of cybersecurity training courses. The Ministry of Interior of the Tuzla Canton mentioned the Turkish Cooperation and Coordination Agency – which is subordinate to the Turkish Ministry of Culture and Tourism.[53]

[50] See: https://www.giz.de/en/html/about_giz.html.
[51] See: https://www.justice.gov/criminal-icitap.
[52] Ministry of Communications and Transport of Bosnia and Herzegovina, "Ministar Mitrović Sa Predstavnicima Huawei," www.mkt.gov.ba, December 1, 2020, http://www.mkt.gov.ba/Publication/Read/ministar-mitrovic-sa-predstavnicima-huaweia.
[53] Turkish Cooperation and Coordination Agency (TİKA), "About Us - TİKA," Tika.gov.tr, 2011, https://www.tika.gov.tr/en/page/about_us-14650.

International organisations

Although partner countries are playing a pivotal role in supporting BiH in the cyber sphere, international organisations are the actors contributing the most in terms of funds and projects. The following are the main international organisations supporting BiH's efforts in the cybersecurity field:

- The Organisation for Security and Co-operation in Europe (OSCE).
- The North Atlantic Treaty Organisation (NATO).
- The United Nations (UN).
- The Council of Europe.
- Other international organisations.

OSCE is playing a crucial role in enhancing BiH's cyber capabilities. Especially, the *Neretva Group*, part of OSCE, has been supporting public-private partnerships (PPPs), information-sharing and cooperation.[54] Moreover, OSCE is organising seminars on cybersecurity with the Ministry of Defence (MoD) to strengthen the country's cyberspatialities and crisis management.[55] The questionnaire's answers have revealed that 8 out of 19 institutions have received trainings courses on cybersecurity offered and organised by OSCE. Finally, the 2019 OSCE's *Guidelines for a Strategic Cybersecurity Framework on Bosnia and Herzegovina* is the most prominent example of the efforts, time, and energy the organisation is employing to support BiH.

Furthermore, NATO, which BiH aims to join, is developing scientific and technological cooperation. Particularly, BiH's experts are being involved in the implementation of the *Next-generation Incident Command System* (NICS) which will facilitate cyber collaboration among Western Balkan countries.[56] Moreover, BiH has been actively engaged with the NATO *Science for Peace and Security (SPC) Programme* since 2007, being involved in scientific cooperation efforts in the field of cybersecurity.[57] The BiH MoD mentioned the Adriatic Charter – an association linked to NATO – as a provider of courses.

Similarly, the UN is strengthening BiH cyberspatialities. As addressed in the previous pages of this report, UNDP's RFF donated $560,183 for the *DigitalBIZ* project which aims to steer BiH's companies towards the digital economy.[58]

[54] Dražen Maravić, "Cybersecurity Policy Development and Capacity Building – Increasing Regional Cooperation in the Western Balkans" (High Level Regional Conference Cyber Resilience and Cybersecurity Capacity Building in the Western Balkans, Geneva Centre for Security Sector Governance (DCAF), 2021), https://www.dcaf.ch/sites/default/files/imce/Events/CybersecurityConference_DiscussionPaperPanel2_PublicCapacityBuildingRegionalCooperation.pdf.

[55] Organisation for Security and Co-operation in Europe (OSCE), "BiH Ministry of Defence and OSCE Mission to BiH Organize 13th Strategic Political-Military Seminar on Cybersecurity and Crisis Management," www.osce.org, December 8, 2021, https://www.osce.org/mission-to-bosnia-and-herzegovina/507446.

[56] North Atlantic Treaty Organisation (NATO), "Relations with Bosnia and Herzegovina," NATO, 2021, https://www.nato.int/cps/en/natohq/topics_49127.htm.

[57] The NATO Science for Peace and Security Programme, "Country Flyer 2021 Bosnia and Herzegovina," 2021, https://www.nato.int/science/country-fliers/BIH.pdf.

[58] United Nations Development Programme (UNDP) in Bosnia and Herzegovina, "Digital Transformation in Business – DigitalBIZ | UNDP in Bosnia and Herzegovina," United Nations Development Programme (UNDP) in Bosnia and Herzegovina, 2020, https://www.ba.undp.org/content/bosnia_and_herzegovina/en/home/development-impact/DigitalBiz.html; United Nations Development Programme (UNDP), "Digital Transformation in Business," Undp.org, 2022, https://open.undp.org/projects/00126505.

Moreover, the UN is providing BiH public institutions with training courses; the Federal Police Administration mentioned the United Nations Development Programme (UNDP) as a provider. Similarly, SIPA mentioned the United Nations Office on Drugs and Crime in its answers on courses providers.

In addition, the Council of Europe is organising workshops and seminars with key BiH public bodies in order to enhance the country's capacity to combat cybercrime.[59] The Council of Europe is supporting BiH public institutions' cyber capabilities, being mentioned by several institutions such as Directorate for Coordination of Police Bodies of BiH, SIPA and the Federal Police Administration. Finally, other international organisations are supporting BiH in the building of cyber capabilities. For instance, SIPA mentioned the Southeast European Law Enforcement Center as a provider.[60] The RS Ministry of Internal Affairs cited INTERPOL as a provider of trainings.

European Union (EU)

The EU is strongly supporting the building of BiH's cyber capabilities. Since the production of the *Western Balkan Strategy* in 2018, cybersecurity has been a key area of cooperation between the EU and its Balkan partners.[61] Through the support offered by the *European Union Agency for Law Enforcement Cooperation* (EUROPOL) and European Network and Information Security Agency (ENISA), the EU aims to strengthen cybers capabilities, especially in the fight against cybercrime, in Western Balkan countries.[62] These goals have been further stated in the 2020 *EU Connectivity Agenda for the Western Balkans*.[63]

Moreover, the EU is providing cyber training to BiH's public employees. For instance, the *European Union Agency for Law Enforcement Training* (CEPOL) has already held seminars to instruct officers and prosecutors on new trends in cyberspace such as the use of cryptocurrencies for illegal purposes.[64] Also, the EU has developed several tools and policies to enhance international cyber cooperation in the field of law enforcement and cyber-criminal justice.[65] As of this, in 2020 the project *EU 4 Fight against Cybercrime in BiH*[66] has been providing the Ministry of Security

[59] Council of Europe, "IPROCEEDS-2: Workshop on Drafting Policies and Strategies on Cybersecurity in Bosnia and Herzegovina," Cybercrime, 2020, https://www.coe.int/en/web/cybercrime/-/iproceeds-2-workshop-on-drafting-policies-and-strategies-on-cybersecurity-in-bosnia-and-herzegovina.

[60] The centre is 'a law enforcement, treaty-based international organization that brings together the resources and expertise of Police and Customs authorities that join synergies in combating more effectively trans-border organized crime in the region.' See: https://www.selec.org/about-selec/.

[61] European Commission, "A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans," 2018, https://ec.europa.eu/info/sites/default/files/communication-credible-enlargement-perspective-western-balkans_en.pdf.

[62] Ibid.

[63] European Commission, "EU Connectivity Agenda for the Western Balkans," 2020, https://ec.europa.eu/neighbourhood-enlargement/system/files/2021-03/brochure_wb_connectivity_agenda_en.pdf.

[64] European Union Agency for Law Enforcement Training (CEPOL), "Crypto Currencies: Investigation Challenges," *CEPOL* (blog), May 29, 2019, https://www.cepol.europa.eu/education-training/what-we-teach/webinars/crypto-currencies-investigation-challenges.

[65] Patryk Pawlak, "Operational Guidance for the EUs International Cooperation on Cyber Capacity Building" (Luxembourg: European Union Institute for Security Studies (EUISS), 2018), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf.

[66] The project is a Twinning action grant. Twinning is a European Union (EU) institution building tool, available to beneficiaries of the Instrument for Pre-Accession Assistance (IPA) and the European Neighbourhood Instrument (ENI). Created in 1998 in the light of the enlargement of the EU, Twinning is based on partnership cooperation between public administrations and accepted mandated bodies of Member States and of a Beneficiary with the purpose of achieving mandatory results/outputs jointly agreed with the Commission. See: European Commission, "Twinning Manual"

with opportunities to better prepare law enforcement agencies, enhance internal and international cooperation, and align the legislation with the Budapest Convention and European good practices.[67] In addition, the EU is providing funds and economic aid for business development to BiH's private sector. For instance, the *EU4Business* project, worth 16.1 million euros, has been providing funds to support and stimulate the development of micro, small and medium-sized companies from April 2018 to March 2022.[68]

Finally, other lesser-known EU projects are in place. BiH public institutions mentioned numerous opportunities provided by the EU. Among others, the Technical Assistance and Information Exchange (TAIEX) instrument of the European Commission, and iPROCEEDS were mentioned as EU-sponsored and -funded projects and programmes assisting BiH public institutions in the building of cyber capabilities.

(European Commission, 2017), https://ec.europa.eu/neighbourhood-enlargement/system/files/2020-09/twinning_manual_2017_update_2020.pdf.

[67] European Commission, "EU 4 Fight against Cybercrime in BiH" (European Commission, 2020), https://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Europa/EU-Twinning/Juli-September_20/EU_4_Fight_against_Cybercrime_in_BiH.pdf.

[68] EU4Business, "EU4Business – for Competitive and Innovative Local Economy," EU4Business, accessed February 28, 2022, https://eu4business.ba/en/.

Policy recommendations

Based on the above analysis, this paper provides policy recommendations clustered in immediate-, near- and long-term objectives. The immediate-term objectives are goals BiH should start pursuing immediately, while near-term objectives shall be achieved in the near future (≈5 years). Long-term objectives are desirable steps to take which, however, can only be achieved if the previous goals are pursued. This analysis suggests the government of BiH:

- In the *immediate-term* **develop a comprehensive approach to cybersecurity**:
    - *Develop a comprehensive cybersecurity framework.*
    - *Establish the state level CERT.*
    - *Produce a national risk assessment to identify cyber CIs.*
    - *Plan cybersecurity crisis management.*
    - *Promote the formation of a cybersecurity culture and mindset in both the public and private sectors.*

- In the *near-term* **develop and implement a national cybersecurity strategy (NCSS) and related policies**:
    - *Enhance cybersecurity awareness.*
    - *Produce a strategy to counter cybercrime.*
    - *Implement and govern the NCSS.*

- In the *long-term* **establish a state agency for cybersecurity**:
    - *Coordinate national cybersecurity efforts.*
    - *Build cyber resilience and promote cyber awareness.*
    - *Refine BiH's cybersecurity architecture.*

The policy recommendations are not mutually exclusive and should be viewed as a multi-level plan to put into place and constantly monitor. The recommendations will be better detailed and addressed in the following sections. All the policy recommendations provided are based on international standards and principles provided by international organisations with a specific focus on European countries and the EU. It is important to note that BiH can and should exploit international cooperation with key partners, both countries and intergovernmental organisations, to achieve the cyber goals and objectives outlined in the policy recommendations.

A comprehensive approach to cybersecurity

In order to develop a comprehensive cybersecurity framework, BiH should design a well-informed plan. In 2019, such a plan has been offered to BiH by the OSCE's *Guidelines for a Strategic Cybersecurity Framework on Bosnia and Herzegovina*.[69] The document is based on the EU's legislation such as the *NIS Directive*, the best practices of European countries, and international standards like the *International Organisation for Standardisation*'s (ISO) 27000 family of standards and ENISA's standards. Therefore, not only does the document provide effective guidelines and a comprehensive framework for cybersecurity, but it can also pave the way for further alignment with international standards.

By providing recommendations based on a multi-stakeholder and whole-of-government approach, the OSCE document states 9 strategic objectives BiH should pursue to develop a comprehensive cybersecurity framework:

[1] A systematic approach to the harmonization and development of cybersecurity legislation;
[2] Secured Information and Communication Systems of the Key Services Providers;
[3] Raising the Awareness and Knowledge of Cybersecurity;
[4] Functional Bodies in charge of Securing, Strengthening and Improving Cybersecurity;
[5] Improved Security and Resilience of Information and Communication Systems;
[6] Enhanced Capacity to Combat Cybercrime;
[7] Effective Cybersecurity Co-operation established in International, Regional and National Frameworks;
[8] Capacity Built to Adequately Respond to Crisis;
[9] Public-Private Partnership Established.

OSCE's recommendations can be summarised and clustered in the following main areas: 1) actions in the legal framework; 2) authorities and responsibilities; 3) cybersecurity awareness; 4) cooperation and implementation.

Actions in the legal framework

The OSCE document suggests a comprehensive review of the current legislation on cybersecurity and related policies, which should be followed by alignment with international standards. Subsequently, key services and databases need to be defined by the legal framework and minimum commonly shared cybersecurity standards need to be developed. This requires a comprehensive risk analysis and assessment. Moreover, BiH should improve and expand its legislation addressing cybercrime, considering new and emerging trends. Finally, resources should be allocated to ensure personnel and technical capabilities for law enforcement to persecute cybercrimes.

[69] Organisation for Security and Co-operation in Europe (OSCE), "Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina," *Www.osce.org* (Organisation for Security and Co-operation in Europe (OSCE), 2019), https://www.osce.org/mission-to-bosnia-and-herzegovina/438383.

Authorities and responsibilities

The document emphasises the necessity to establish a national *Computer Security Incident Response Team* (CSIRT). It highlights and mentions the required key service sectors, the key service providers and the requirements and tasks of CSIRTs under the *NIS Directive*,[70] thus offering international standards and good practices BiH needs to align with, especially in light of its objective to join the EU. These recommendations can respond not only to the necessity of establishing an effective and efficient state level CERT but also to BiH's international commitments and aspirations. Indeed, developing a cybersecurity framework which respects the standards and principles of the EU and European countries can facilitate BiH's access to the EU.

Moreover, authorities in charge of ICTs security need to cover key services such as energetics, transportation, and banking. A point of contact for the international cooperation of these competent authorities should be established. In addition, it is necessary for CRA to ensure that providers of communication services enforce the cyber protection of their systems. Finally, BiH should select *cloud computing* providers that meet international standards, define them, and decide what data shall and shall not be sent to the *cloud* outside the country.

Cybersecurity awareness

The document dedicates particular attention to cybersecurity awareness in both the public and private sectors. As of this, it is necessary to design, develop and offer training programmes and workshops – to be mandatory for public employees – to raise cybersecurity awareness in society and public institutions. Especially, officers, prosecutors and judges should be offered trainings and courses on cybercrime. Finally, it is important to encourage and finance research and development in the field of cybersecurity across both the public and private sectors.

Cooperation and implementation

The country should develop domestic cooperation between the different agencies and bodies in charge of cybersecurity as well as engage in international and regional cooperation in the field. In addition, it is important to develop public-private partnerships (PPPs) in order to develop cybersecurity products and services, improve information-sharing among different partners, and meet international standards. As of this, the OSCE document mentions the *Public Private Partnerships (PPP) Cooperative models* published in 2017 by ENISA as a framework to adopt.[71]

Finally, special attention is dedicated to the implementation of the cybersecurity framework through crisis management. It is necessary to establish criteria for crisis identification and reporting incidents mechanisms. CSIRTs play an essential role as the primary subjects incidents should be reported to. Ministries and responsible bodies should also outline clear plans and procedures to follow should crises break out.

[70] Ibid.

[71] European Network and Information Security Agency (ENISA), "Public Private Partnerships (PPP) - Cooperative Models" (European Network and Information Security Agency (ENISA), 2017), Public Private Partnerships (PPP) Cooperative models.

National cybersecurity strategy and related policies

National cybersecurity strategies are key components for a nation to improve its security and address cyber threats.[72] Since 2017, all EU members states have developed, adopted and published their national cybersecurity strategies as required by the *NIS Directive*.[73] These documents and the ENISA's reports, guides and policy recommendations can provide BiH with a set of good practices, principles and standards to adopt in order to design, develop and implement an effective and comprehensive NCSS.

The design and development of NCSS

ENISA has published a practical guide to developing national cybersecurity strategies based on a set of recognised good practices from European countries, desk analysis and interviews with public stakeholders.[74] The guide overlaps with some of the observations made by the 2019 OSCE document but link them to the development and implementation of a national cybersecurity strategy.

According to the guide, there are 6 main steps to design and develop a comprehensive and effective national cybersecurity strategy:

1. Set the vision, scope, objectives, and priorities.
2. Follow a risk assessment approach.
3. Take stock of existing policies, regulations, and capabilities.
4. Set a clear governance structure.
5. Identify and engage stakeholders.
6. Establish trusted information-sharing mechanisms.

Hence, an effective BiH's NCSS should define the vision and scope by establishing national objectives to accomplish in a specific timeframe, identify the sectors in scope, set priorities, and design a roadmap for the implementation of the strategy. However, this is not sufficient. Indeed, the future NCSS needs to provide a national risk assessment based on a scientific and technological process which focuses on cyber critical infrastructures and assets and aims at risk identification, risk analysis and risk evaluation.

Moreover, additional steps are needed to develop the NCSS. It is necessary to consider already existing policies and international laws and standards that must be incorporated into the strategy. It is then pivotal to define roles, responsibilities, and accountabilities of stakeholders, establishing a governmental working group in charge of coordinating the efforts to produce the strategy.

[72] Kevin P. Newmeyer, "Elements of National Cybersecurity Strategies for Developing Nations," *National Cybersecurity Institute Journal* 1, no. 3 (2015): 9–19, http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf#page=11.

[73] European Network and Information Security Agency (ENISA), "National Cyber Security Strategies - Interactive Map," www.enisa.europa.eu (European Network and Information Security Agency (ENISA), n.d.), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

[74] European Network and Information Security Agency (ENISA), *NCSS Good Practice Guide : Designing and Implementing National Cyber Security Strategies.* (Heraklion: ENISA, 2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Finally, to be comprehensive, an effective cyber strategy must involve the private sector in the process through PPPs and information-sharing mechanisms between the public and private sectors.

Although European countries and ENISA can offer fundamental reflections and documental sources to BiH, they are not the sole examples the country could derive inspiration from. Indeed, numerous non-European countries such as the United States,[75] Canada,[76] Japan[77] and Israel[78] have developed, published, and implemented their national NCSSs. Nonetheless, it is important to bear in mind that the European documents are based also on the EU's laws, regulations, and recommendations. Therefore, they can provide BiH with precious sources to consider in light of the country's desire to access the EU.

Cybersecurity awareness as a key component of NCSS

ENISA retains cybersecurity awareness as a key component of NCSS. In 2021 the agency published the report *Raising Awareness of Cybersecurity* which, based on desk analysis and interviews conducted with key public bodies in charge of cybersecurity in 20 European countries, aims to present good practices concerning the incorporation of cyber awareness into NCSS.[79] The report provides a guide to design, develop, and implement effective cyber awareness programmes and enhance NCSSs.

According to the report, it is first necessary to provide the NCSS with a clear vision of cyber awareness, defining why it is needed, what objectives are to be accomplished, and to whom it applies. Secondly, it is fundamental to identify the public and private bodies that will coordinate and cooperate within the nation to conduct cybersecurity awareness activities. Generally, European countries tend to charge one main public body of cyber awareness campaigns. However, countries such as Finland, Luxembourg and the Netherlands adopted a different approach with multiple entities carrying out cybersecurity awareness activities. Furthermore, it is important to allocate and define the resources (e.g., budget, and personnel) to employ for cybersecurity awareness campaigns. As of this, ENISA notes that European funds are available and already being used by numerous countries.

In addition, the agencies in charge of cybersecurity need to cooperate with the media, especially to tackle misinformation and disinformation, two prominent cyber threats. Moreover, it is necessary to inform the wider public about cybersecurity trends and challenges through the publication of reports that promote awareness and public discussion. Cybersecurity awareness measurements should be conducted through public surveys to identify gaps that need to be filled. With concern to this, public bodies should cooperate with national statistics offices to conduct effective surveys.

[75] The White House, "National Cyber Strategy of the United States," 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[76] Public Safety Canada, *National Cyber Security Strategy : Canada's Vision for Security and Prosperity in the Digital Age* (Ottawa, Ontario: Public Safety Canada, 2018).

[77] The Government of Japan, "Cybersecurity for All," 2021, https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021-en-booklet.pdf.

[78] Prime Minister's Office, "Israel National Cyber Security Strategy in Brief," 2017, https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

[79] European Network and Information Security Agency (ENISA), "Raising Awareness of Cybersecurity" (European Network and Information Security Agency (ENISA), 2021), https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity.

Finally, the planning of cybersecurity awareness campaigns plays a crucial role and should be defined in terms of target groups, channels to reach the audiences, performance indicators and regular monitoring.

The fight against cybercrime

Not only ENISA's documents but also European and non-European countries' strategies emphasise the importance of the fight against cybercrime, dedicating attention to it in their NCSSs. The above-mentioned 2019 OSCE document highlights the importance of such aspects as well. As of cybercrime, BiH needs to take further steps to design an effective strategy; particularly, BiH must further implement the Budapest Convention as the treaty is legally binding.

In 2021, the *International Criminal Police Organisation* (INTERPOL) has produced a guide to design strategies to fight cybercrime that BiH could use to develop its own.[80] According to the report, a cybercrime strategy presents 4 main components:

1. Introduction.
2. Current cybercrime landscape – assessment and analysis.
3. Vision.
4. Focus Areas, Strategic Objectives and Action Items.

BiH' strategy should explain the reasons behind the development of the strategy, emphasising why it is necessary and how it will help the nation. Subsequently, the document should provide the definition of cybercrime the government adopts, cybercrime statistics, an overview of legislation and strategies concerning cybercrime, the authorities in charge of fighting cybercrime, and, finally, a self-assessment of the cyber capabilities to combat cybercrime. The document should then set the vision which includes the desired successes to achieve in the fight against cybercrime. Finally, the strategy should establish what objectives and goals to achieve in a certain timeframe, individual deadlines, performance indicators, and monitoring measures.

A potential cybercrime strategy can take different forms as demonstrated by the strategies developed in different countries. It can be incorporated into the national cybersecurity strategy as in Australia[81] and the United Kingdom[82] or it can be developed as a separate document like in New Zealand.[83] In addition, the strategy does not necessarily need to be produced by the higher levels of the government. For instance, the Canadian strategy was produced by the *Royal Canadian Mounted Police*.[84]

[80] International Criminal Police Organisation (INTERPOL), "National Cybercrime Strategy Guidebook" (International Criminal Police Organisation (INTERPOL), 2021), file:///C:/Users/HP/Downloads/National%20Cybercrime%20Strategy%20Guidebook%20(1).pdf.

[81] Department of Home Affairs, "Australia's Cyber Security Strategy," 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

[82] Her Majesty's Government, "National Cyber Strategy 2022," 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

[83] Security and Intelligence Group (SIG), "National Plan to Address Cybercrime," 2015, https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy.

[84] Royal Canadian Mounted Police (RCMP), "Royal Canadian Mounted Police Cybercrime Strategy," 2015, https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf.

Besides this minor aspect, developing and implementing a cybercrime strategy is pivotal for BiH in order to align with the principles and standards set by the *Convention on Cybercrime of the Council of Europe*.[85] As BiH signed and ratified the treaty which poses legal obligations for the country,[86] the development of a strategy to fight cybercrime assumes increased importance.

Moreover, BiH should pay particular attention to new and emerging trends in cybercrime. For example, the author of this report detected a gap concerning the potential criminal and terrorist use of cryptocurrencies which is not addressed in BiH's official documents. The 2020 *Assessment of Risk of Money Laundering and Financing of Terrorism in BiH for the Period from 2018 to 2022* does not mention the cyber dimension of money laundering,[87] overlooking the potential use of cryptocurrencies for money laundering and financing. Although BiH does not recognise cryptocurrencies as legal tenders, cryptocurrencies are being traded in BiH.[88] The lack of regulation over this cutting-edge technology results detrimental, especially because cryptocurrencies are being increasingly used by criminal organisations in the country.[89]

Numerous studies on the terrorist use of cryptocurrencies exist and BiH public institutions should examine these sources to address the issue. Particularly, jihadi terrorist groups like *Al-Qaeda* and the *Islamic State* are using cryptocurrencies for illicit purposes.[90] Hence, it is necessary for the country to evaluate whether the terrorist use of cryptocurrencies is affecting or could affect BiH and take action. As of this, the *Financial Action Task Force* (FATF) has published several reports, providing recommendations concerning virtual assets, money laundering and terrorist financing.[91] Furthermore, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) of the Council of Europe, that BiH is part of, published a 2021 report which outlines guidelines to counter the issue of criminal and terrorist financing

[85] International Criminal Police Organisation (INTERPOL), "National Cybercrime Strategy Guidebook" (International Criminal Police Organisation (INTERPOL), 2021), file:///C:/Users/HP/Downloads/National%20Cybercrime%20Strategy%20Guidebook%20(1).pdf.

[86] Organisation for Security and Co-operation in Europe (OSCE), "Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina," *Www.osce.org* (Organisation for Security and Co-operation in Europe (OSCE), 2019), https://www.osce.org/mission-to-bosnia-and-herzegovina/438383.

[87] Ministry of Security of Bosnia and Herzegovina, "Assessment of Risk of Money Laundering and Financing of Terrorism in BiH for the Period from 2018 to 2022," 2018, http://www.msb.gov.ba/PDF/120620205.pdf.

[88] Maja Nišević, Chiara Zamboni, and Bojan Kovačević, "Cryptocurrencies: Highlighting the Perspective of Bosnia and Herzegovina," *International Review of Law, Computers & Technology*, December 2, 2021, 1–20, https://doi.org/10.1080/13600869.2021.2004759.

[89] Nikolina Maleta and Ivana Stipanovic, "Difficulties in Procedure of Obtaining Evidence on Money Laundering through Cryptocurrencies as a Possible Threat to the Market Stability," in *Economic and Social Development (Book of Proceedings), 31st International Scientific Conference on Economic and Social Development - "Legal Challenges of Modern World,"* ed. Marijan Cingula, Douglas Rhein, and Mustapha Machrafi, 2018, https://is.muni.cz/repo/1420998/Book_of_Proceedings_esdSplit2018_Online.pdf#page=598.

[90] The Soufan Center, "IntelBrief: Terrorists' Use of Cryptocurrency," *The Soufan Center* (blog), December 10, 2020, https://thesoufancenter.org/intelbrief-2020-december-10/; Shacheng Wang and Xixi Zhu, "Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing," *Policing: A Journal of Policy and Practice* 15, no. 4 (September 7, 2021), https://doi.org/10.1093/police/paab059.

[91] The Financial Action Task Force (FATF), "Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets" (The Financial Action Task Force (FATF), 2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf; The Financial Action Task Force (FATF), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" (The Financial Action Task Force (FATF), 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

through cryptocurrencies.[92] These sources can offer BiH recommendations to design and implement measures to tackle the criminal and terrorist use of cryptocurrencies. Moreover, developing such measures will result fundamental for the country to adopt the EU's legislation on the matter such as the 2019 *Directive on non-cash payment*.[93]

Although these steps are fundamental elements to develop a cybercrime strategy, cyber awareness and cyber trainings constitute the baseline to effectively implement these measures. The necessity of cybersecurity awareness and education in the fight against cybercrime is deemed to be critical for BiH.[94] This applies not only to citizens but also to governmental bodies supporting BiH's cyber-policies. Researchers have noted that the Centre for Education of Judges and Prosecutors and Judicial Commission of BD does not provide cybercrime-related programmes.[95] Hence, an effective cybercrime strategy would require BiH to provide its public employees and law enforcement and justice system agencies and bodies with cyber training on cybercrime. Citizens as well need to develop more enhanced cyber awareness as they are key targets of cybercrime.

Implementing and governing NCSS

Once developed, the national cybersecurity strategy needs to be governed. As of this, ENISA provides an effective managing approach which outlines the NCSS's lifecycle (Figure 4).[96]

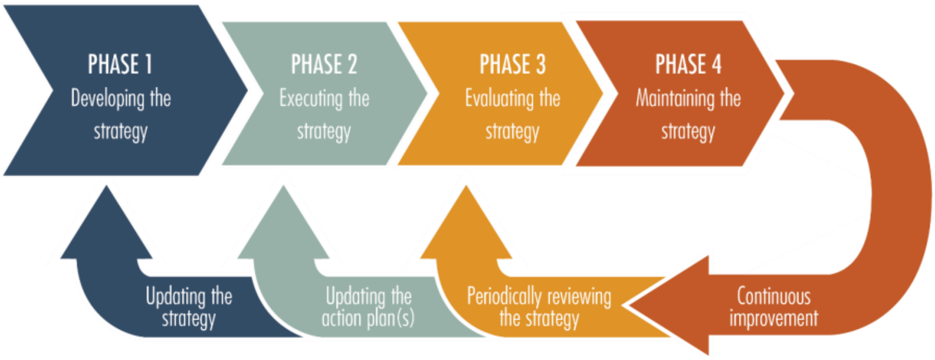


Figure 4. *National cybersecurity strategy's lifecycle*

After developing and executing the NCSS, it is necessary to evaluate whether its objectives have been achieved. The ENISA assessment framework allows for conducting such an evaluation through the analysis of the NCSS and of the country's cyber capabilities and the identification of areas for improvement.[97]

[92] Cybercrime Programme Office of the Council of Europe, "Guide on Seizing Cryptocurrencies" (Council of Europe, 2021), https://rm.coe.int/0900001680a2276b.

[93] European Parliament and The Council, "Directive on Non-Cash Payment," DIRECTIVE (EU) 2019/713 § (2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN.

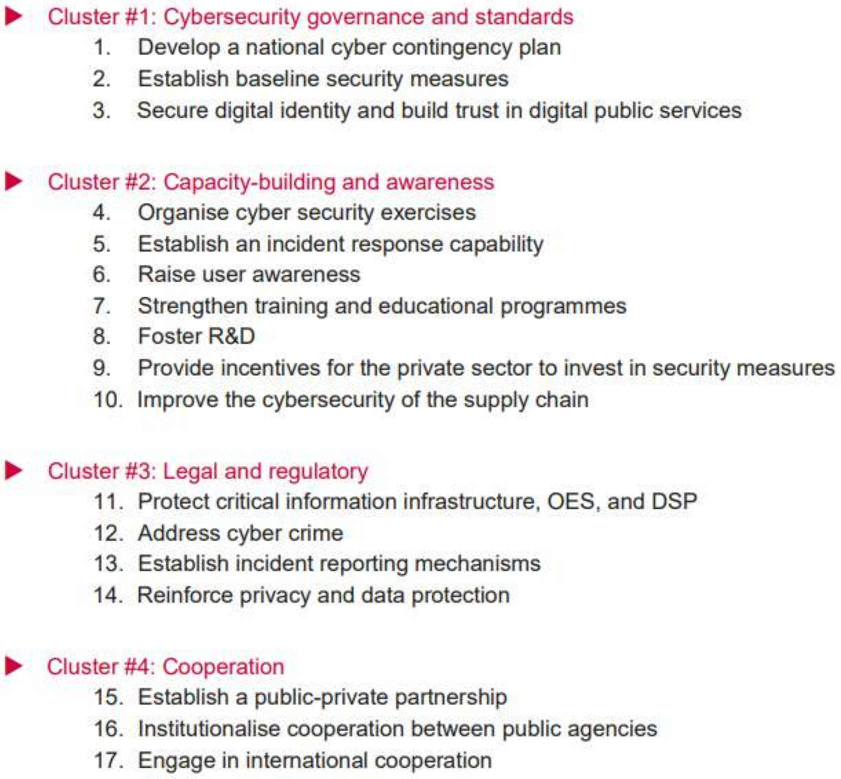
[94] Sabina Baraković and Jasmina Baraković Husić, "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina," *Information & Security: An International Journal* 32 (2015): 131–54, https://doi.org/10.11610/isij.3205.

[95] Ibid.

[96] European Network and Information Security Agency (ENISA), *NCSS Good Practice Guide : Designing and Implementing National Cyber Security Strategies.* (Heraklion: ENISA, 2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[97] European Network and Information Security Agency (ENISA), "National Capabilities Assessment Framework" (European Network and Information Security Agency (ENISA), 2020), https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework.

The ENISA's report, like the other agency's documents mentioned previously, is based on desk analysis, interviews with key stakeholders and best practices of European countries, thus offering BiH a core document to consider when addressing cybersecurity. The report provides a National Capabilities Assessment Framework (NCAF) which covers 17 strategic objectives and is structured around 4 main clusters (Figure 5).[98]



▶ Cluster #1: Cybersecurity governance and standards

1. Develop a national cyber contingency plan
2. Establish baseline security measures
3. Secure digital identity and build trust in digital public services

▶ Cluster #2: Capacity-building and awareness

4. Organise cyber security exercises
5. Establish an incident response capability
6. Raise user awareness
7. Strengthen training and educational programmes
8. Foster R&D
9. Provide incentives for the private sector to invest in security measures
10. Improve the cybersecurity of the supply chain

▶ Cluster #3: Legal and regulatory

11. Protect critical information infrastructure, OES, and DSP
12. Address cyber crime
13. Establish incident reporting mechanisms
14. Reinforce privacy and data protection

▶ Cluster #4: Cooperation

15. Establish a public-private partnership
16. Institutionalise cooperation between public agencies
17. Engage in international cooperation

Figure 5. *The 17 objectives covered by the NCAF developed by ENISA.*

An agency for national cybersecurity

A final step BiH should take in the future is to create an agency for national cybersecurity. Multiple countries in the world have agencies or governmental bodies charged of cybersecurity. For instance, France, Finland, and Germany have developed cybersecurity agencies or centres.[99] Similarly, non-European countries, from the United States[100] to Singapore,[101] present cybersecurity agencies and centres. These governmental entities serve numerous purposes, including coordination between different national agencies and between public bodies and the private sector, the production of strategic documents, and the development of cyber awareness campaigns.

[98] Ibid.

[99] Olga Vakulyk et al., "Cybersecurity as a Component of the National Security of the State," *Journal of Security and Sustainability Issues* 9, no. 3 (March 25, 2020): 775–84, https://doi.org/10.9770/jssi.2020.9.3(4).

[100] Cybersecurity & Infrastructure Security Agency (CISA), "ABOUT CISA | CISA," Cisa.gov, 2018, https://www.cisa.gov/about-cisa.

[101] Cyber Security Agency of Singapore (CSA), "Cyber Security Agency of Singapore (CSA)," Cyber Security Agency (CSA), 2019, https://www.csa.gov.sg/.

There are numerous examples among Western and non-Western countries that can provide BiH with good practices and standards for establishing and organising an agency for national cybersecurity. A recent example can be found in Italy. In 2021, the Italian government established the Agency for National Cybersecurity (*Agenzia per la cybersicurezza nazionale* (ACN)) by *Decree-Law 14th of June, no. 82.*[102] According to the legislation, the creation of the agency serves the following main purposes:[103]

- To address the vulnerabilities ICTs can suffer and their impact on both the public and private sectors.
- To reassign competencies in the field of cybersecurity and ensure more efficient coordination.
- To build a more resilient and secure country in cyberspace.
- To enact the *Recovery and Resilience Plan* (RRP)[104] by employing its resources to strengthen the economic sector in the field of cybersecurity.
- To redefine the Italian cybersecurity architecture.

The main functions and goals of the agency are the support to public and private actors to prevent cyber incidents, the achievement of national and European strategic autonomy in the digital sphere, and the promotion of cybersecurity culture and awareness.[105] To achieve these objectives, the agency presents a clear organisational structure:[106]

1. The national CSIRT monitors cyber incidents, raises early warnings and alerts, intervenes when incidents occur, analyses risks, and enhances cyber awareness.[107]
2. The *National Assessment and Certification Centre* evaluates and assesses ICT goods, systems and services deemed to be essential.[108]
3. The *National Coordination Centre for cybersecurity* develops European development programmes to improve national cyber capabilities.[109]

The General Director of the agency is named by the Prime Minister, represents the agency and acts as secretary of the *Interministerial Committee for Cybersecurity*, under the *Presidency of the Council of Ministers*, that provides advice and support and monitors the cybersecurity policies.

[102] Agenzia per la Cybersicurezza Nazionale (ACN), "Agenzia per La Cybersicurezza Nazionale [Agency for National Cybersecurity]," www.acn.gov.it, accessed March 2, 2022, https://www.acn.gov.it/.

[103] Presidenza del Consiglio dei Ministri, "DECRETO-LEGGE 14 Giugno 2021, N. 82 [Decree-Law 14th of June 2021, No. 82]," www.normattiva.it, 2021, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14.

[104] The *Recovery and Resilience Plan* (RRP) is an Italian national plan to re-boost the economy after the Covid-19 pandemic. RRP is part of the European Union (EU) programme *Next Generation EU* which allocates a total of 750 billion euros for European recovery after the pandemic and assigned to Italy a total of 191.5 billion euros. See: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698847#:~:text=In%20absolute%20figures%2C%20Italy%27s%20Recovery,)%2C%20including%20its%20loan%20component.

[105] Agenzia per la Cybersicurezza Nazionale (ACN), "Chi Siamo - Agenzia per La Cybersicurezza Nazionale [Who We Are - Agency for National Cybersecurity]," www.acn.gov.it, accessed March 2, 2022, https://www.acn.gov.it/chi-siamo

[106] Ibid.

[107] Computer Security Incident Response Team (CSIRT), "CSIRT Italia [CSIRT Italy]," csirt.gov.it, accessed March 2, 2022, https://csirt.gov.it/chi-siamo.

[108] Ministry of Economic Development, "Centro Di Valutazione E Di Certificazione Nazionale (CVCN) [National Assessment and Certification Centre]," Ministry of Economic Development, accessed March 2, 2022, https://atc.mise.gov.it/index.php/sicurezza/cvcn.

[109] Agenzia per la Cybersicurezza Nazionale (ACN), "Agenzia per La Cybersicurezza Nazionale [Agency for National Cybersecurity]," www.acn.gov.it, accessed March 2, 2022, https://www.acn.gov.it/.

The agency was created to meet pivotal necessities such as the design and development of future national cybersecurity strategies, the function of point of contact, and the need to certify cyber infrastructures and assets. Most importantly, the agency has already accomplished fundamental objectives. For instance, in 2021, the agency, together with the *Department for Digital Transformation*, published the national strategy for the *cloud*.[110] Currently, this governmental body is expanding its resources and staff to fulfil its objectives and further support Italian cyber capabilities.

BiH could take the Italian case as an example to develop its own agency for cybersecurity in the long-term. Such a body would facilitate the coordination between the different governmental institutions and play a fundamental role in the production of cyber strategies and policies, thus centralising the efforts in the cybersecurity field. However, the development of this agency needs to be preceded by the achievement of the *immediate-term* and *near-term* objectives. Otherwise, the agency would not function properly, and its establishment could constitute a waste of sources, energy, and time. If the *immediate*- and *near-term* objectives are accomplished, the creation of the agency for national cybersecurity could be a pivotal tool to further implement the policies previously adopted.

[110] Dipartimento per la Trasformazione Digitale and Agenzia per la Cybersicurezza Nazionale, "Strategia Cloud Italia [Strategy Cloud Italy]," 2021, https://assets.innovazione.gov.it/1634299755-strategiacloudit.pdf.

Conclusions and recommendations for future research

Cybersecurity is a strategic domain for BiH, impacting numerous sectors of society, ranging from the economy to law enforcement. However, BiH's cyber capabilities are underdeveloped and there is a need for their overall improvement. BiH's need to strengthen its cybersecurity stems from the imperative to ensure national security and public safety, mitigate cyber threats, achieve international goals such as accessing the EU and NATO and meet international commitments.

Although BiH has developed core legislation to address cybersecurity issues and its public institutions are acting to mitigate cyber threats such as cybercrime, key gaps in cyber capabilities remain. Particularly, a state CERT has not been developed yet, thus undermining cybersecurity and hindering efforts to address cyber threats and improve cyber capabilities. Moreover, the country has not developed neither a state level cybersecurity strategy nor a strategy against cybercrime. In addition, public institutions are not conducting risk assessments of cyber CIs and cybersecurity drills are almost inexistent. As a result, BiH's approach to cybersecurity is jeopardised and lacks a well-informed and comprehensive framework. There is a low level of cyber awareness in both the public and private sectors, thus exposing institutions, citizens, and private companies to cyber threats and risks.

Hence, BiH must take further steps to enhance its cybersecurity capabilities. Particularly, BiH policymakers should develop a comprehensive approach to cybersecurity by harmonising legislation and aligning it with international standards, establishing a state CERT, conducting risk assessments of cyber CIs, and increasing general cyber awareness in both the public and private sectors. In addition, BiH political leadership needs to produce a national cybersecurity strategy to direct the country's efforts in the cyberspace, strengthen the cybersecurity architecture and pave the way for future reforms and strategies. Finally, BiH decisionmakers should consider the establishment of a state agency for cybersecurity to coordinate cyber efforts, promote cyber awareness and refine the state cybersecurity architecture.

There is a need for further research to comprehensively analyse other facets of cybersecurity in BiH. Particularly, future studies should focus on four main areas of analysis. Firstly, research needs to address the military and intelligence dimension of cybersecurity in BiH, especially considering BiH's goal to become a NATO member. Secondly, scholars should comprehensively analyse the role the EU and European countries can play in strengthening BiH's cyber capabilities, focusing especially on the legal sphere and the adoption of the EU's laws, standards, and principles. Thirdly, researchers should explore the importance of cybersecurity in BiH's industrial sector, paying particular attention to the development of indigenous cyber firms that can support the country's efforts in the building of cyber capabilities. Fourthly, future studies should concentrate on BiH citizens' cyber awareness, online safety, and digital rights as well as on dynamics such as online hate speech and terrorist radicalisation affecting BiH individuals on social media. Future work should adopt methodologies other than desk analysis such as interviews and public surveys to identify key gaps in other sectors of society like the economy, healthcare, and the industrial sector.

Lastly, future research should also consider BiH’s cybersecurity within the broader Western Balkans’ (geo)political landscape. Specifically, it is pivotal to compare BiH’s cyber capabilities development with other Western Balkan countries’ cyber capabilities, exploring gaps and opportunities for international cooperation. Once more, given the objective of numerous Western Balkan countries to join both the EU and NATO, comparative research on BiH’s cybersecurity can allow to find undetected gaps, explore new cooperation opportunities, and further support BiH’s international aspirations.

Bibliography

Agenzia per la Cybersicurezza Nazionale (ACN). "Agenzia per La Cybersicurezza Nazionale [Agency for National Cybersecurity]." www.acn.gov.it. Accessed March 2, 2022. https://www.acn.gov.it/.

———. "Chi Siamo - Agenzia per La Cybersicurezza Nazionale [Who We Are - Agency for National Cybersecurity]." www.acn.gov.it. Accessed March 2, 2022. https://www.acn.gov.it/chi-siamo.

Attorney-General's Department. "National Plan to Combat Cybercrime." Canberra: Commonwealth Of Australia, 2013. https://www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime.pdf.

Baraković, Sabina, and Jasmina Baraković Husić. "'We Have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina." *Information & Security: An International Journal* 32 (2015): 131–54. https://doi.org/10.11610/isij.3205.

Bosnia and Herzegovina Council of Ministers. "Action Plan for Child Protection and Prevention of Violence against Children through Information-Communications Technologies in Bosnia and Herzegovina 2014-2015," 2014. http://msb.gov.ba/PDF/140605_Nasilje_engleski_SG_ver2.pdf.

———. "Strategy for Fight against Organised Crime in Bosnia and Herzegovina (2017-2020)," 2017. http://www.msb.gov.ba/PDF/strategy11122017.pdf.

———. "Strategy of Bosnia and Herzegovina for Preventing and Combating Terrorism 2015-2020." Bosnia and Herzeoginva Council of Ministers, 2015. http://msb.gov.ba/PDF/STRATEGIJA_ZA_BORBU_PROTIV_TERORIZMA_ENG.pdf.

Central European Initiative (CEI). "CEI Plan of Action 2021-2023." Central European Initiative (CEI), 2020. https://www.cei.int/sites/default/files/publications/downloads/CEI%20Plan%20of%20Action%20DIGITAL%20ESEC%20FINAL.pdf.

CERT Republic of Srpska. "Republic of Srpska National CERT | About." CERTRS.org, July 8, 2019. https://certrs.org/en/about/.

Choucri, Nazli. Cyberpolitics in International Relations. Mit Press, 2012.

Civil Society & Think Tank Forum. "Policy Recommendations," 2021. https://wb-csf.eu/docs/Final-Recommendations-CSF2021.pdf.

Clough, Jonathan. "The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World." *Criminal Law Forum* 23, no. 4 (September 25, 2012): 363–91. https://doi.org/10.1007/s10609-012-9183-3.

Communications Regulatory Agency of Bosnia and Herzegovina (CRA). "Annual Report of the Communications Regulatory Agency for 2020." Communications Regulatory Agency of Bosnia and Herzegovina (CRA), 2020. https://docs.rak.ba//documents/f8910d22-e538-4b11-9b21-4f7cfd0e0b88.pdf.

Computer Security Incident Response Team (CSIRT). “CSIRT Italia [CSIRT Italy].” csirt.gov.it. Accessed March 2, 2022. https://csirt.gov.it/chi-siamo.

Council of Europe. “Bosnia and Herzegovina. Octopus Cybercrime Community,” 2017. https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/AZnxfNT8Y3Zl/content/bosnia-and-herzegovina?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-wiki%3Fp_p_id%3D101_INSTANCE_AZnxfNT8Y3Zl%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_pos%3D1%26p_p_col_count%3D2?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2.

———. “IPROCEEDS-2: Workshop on Drafting Policies and Strategies on Cybersecurity in Bosnia and Herzegovina.” Cybercrime, 2020. https://www.coe.int/en/web/cybercrime/-/iproceeds-2-workshop-on-drafting-policies-and-strategies-on-cybersecurity-in-bosnia-and-herzegovina.

Cyber Security Agency of Singapore (CSA). “Cyber Security Agency of Singapore (CSA).” Cyber Security Agency (CSA), 2019. https://www.csa.gov.sg/.

Cybercrime Programme Office of the Council of Europe. “Guide on Seizing Cryptocurrencies.” Council of Europe, 2021. https://rm.coe.int/0900001680a2276b.

Cybersecurity & Infrastructure Security Agency (CISA). “ABOUT CISA | CISA.” Cisa.gov, 2018. https://www.cisa.gov/about-cisa.

Department of Home Affairs. “Australia’s Cyber Security Strategy,” 2020. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Dipartimento per la Trasformazione Digitale, and Agenzia per la Cybersicurezza Nazionale. “Strategia Cloud Italia [Strategy Cloud Italy],” 2021. https://assets.innovazione.gov.it/1634299755-strategiacloudit.pdf.

Eriksson, Johan, and Giampiero Giacomello. “The Information Revolution, Security, and International Relations: (IR)Relevant Theory?” International Political Science Review 27, no. 3 (July 2006): 221–44. https://doi.org/10.1177/0192512106064462.

EU4Business. “EU4Business – for Competitive and Innovative Local Economy.” EU4Business. Accessed February 28, 2022. https://eu4business.ba/en/.

European Commission. “A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans,” 2018. https://ec.europa.eu/info/sites/default/files/communication-credible-enlargement-perspective-western-balkans_en.pdf.

———. “Bosnia and Herzegovina 2021 Report,” 2021. file:///C:/Users/HP/Downloads/Bosnia%20and%20Herzegovina%202021%20report.PDF.

———. "EU 4 Fight against Cybercrime in BiH." European Commission, 2020. https://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Europa/EU-Twinning/Juli-September_20/EU_4_Fight_against_Cybercrime_in_BiH.pdf.

———. "EU Connectivity Agenda for the Western Balkans," 2020. https://ec.europa.eu/neighbourhood-enlargement/system/files/2021-03/brochure_wb_connectivity_agenda_en.pdf.

———. "Twinning Manual." European Commission, 2017. https://ec.europa.eu/neighbourhood-enlargement/system/files/2020-09/twinning_manual_2017_update_2020.pdf.

European Network and Information Security Agency (ENISA). "National Capabilities Assessment Framework." European Network and Information Security Agency (ENISA), 2020. https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework.

———. "National Cyber Security Strategies - Interactive Map." www.enisa.europa.eu. European Network and Information Security Agency (ENISA), n.d. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

———. *NCSS Good Practice Guide : Designing and Implementing National Cyber Security Strategies*. Heraklion: ENISA, 2016. https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

———. "Public Private Partnerships (PPP) - Cooperative Models." European Network and Information Security Agency (ENISA), 2017. Public Private Partnerships (PPP) Cooperative models.

———. "Raising Awareness of Cybersecurity." European Network and Information Security Agency (ENISA), 2021. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity.

European Parliament, and The Council. Directive on non-cash payment, DIRECTIVE (EU) 2019/713 § (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN.

European Union Agency for Law Enforcement Training (CEPOL). "Crypto Currencies: Investigation Challenges." *CEPOL* (blog), May 29, 2019. https://www.cepol.europa.eu/education-training/what-we-teach/webinars/crypto-currencies-investigation-challenges.

Her Majesty's Government. "National Cyber Strategy 2022," 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

High Judicial and Prosecutorial Council of Bosnia and Herzegovina. "Politika Sigurnosti Pravosudnog Informacionog Sistema Bosne I Hercegovine [Security Policy of the Judicial Information System of Bosnia and Herzegovina]." High Judicial and Prosecutorial Council of Bosnia and Herzegovina, 2016. https://portalfo1.pravosudje.ba/vstvfo-api/vijest/download/44943.

International Criminal Police Organisation (INTERPOL). “National Cybercrime Strategy Guidebook.” International Criminal Police Organisation (INTERPOL), 2021. file:///C:/Users/HP/Downloads/National%20Cybercrime%20Strategy%20Guidebook%20(1).pdf.

International Telecommunication Union (ITU). “Bosnia and Herzegovina.” www.itu.int. Accessed February 28, 2022. https://www.itu.int/online/mm/scripts/gensel9?_ctryid=1000100548.

Maleta, Nikolina, and Ivana Stipanovic. “Difficulties in Procedure of Obtaining Evidence on Money Laundering through Cryptocurrencies as a Possible Threat to the Market Stability.” In *Economic and Social Development (Book of Proceedings), 31st International Scientific Conference on Economic and Social Development - “Legal Challenges of Modern World,”* edited by Marijan Cingula, Douglas Rhein, and Mustapha Machrafi, 2018. https://is.muni.cz/repo/1420998/Book_of_Proceedings_esdSplit2018_Online.pdf#page=598.

Maravić, Dražen. “Cybersecurity Policy Development and Capacity Building – Increasing Regional Cooperation in the Western Balkans.” Geneva Centre for Security Sector Governance (DCAF), 2021. https://www.dcaf.ch/sites/default/files/imce/Events/CybersecurityConference_DiscussionPaperPanel2_PublicCapacityBuildingRegionalCooperation.pdf.

Mastracci, Matteo. “Wave of Cyber Crimes, Political Clashes, Buffets Region.” Balkan Insight, February 18, 2022. https://balkaninsight.com/2022/02/18/wave-of-cyber-crimes-political-clashes-buffets-region/.

Metodieva, Asya. “The Radical Milieu and Radical Influencers of Bosnian Foreign Fighters.” Studies in Conflict & Terrorism, January 18, 2021, 1–21. https://doi.org/10.1080/1057610x.2020.1868097.

Ministry of Communications and Transport of Bosnia and Herzegovina. “Ministar Mitrović Sa Predstavnicima Huaweia.” www.mkt.gov.ba, December 1, 2020. http://www.mkt.gov.ba/Publication/Read/ministar-mitrovic-sa-predstavnicima-huaweia.

Ministry of Economic Development. “Centro Di Valutazione E Di Certificazione Nazionale (CVCN) [National Assessment and Certification Centre].” Ministry of Economic Development. Accessed March 2, 2022. https://atc.mise.gov.it/index.php/sicurezza/cvcn.

Ministry of Security of Bosnia and Herzegovina. “Assessment of Risk of Money Laundering and Financing of Terrorism in BiH for the Period from 2018 to 2022,” 2018. http://www.msb.gov.ba/PDF/120620205.pdf.

———. “Strategy for Establishing CERT in Bosnia and Herzegovina.” Ministry of Security of Bosnia and Herzegovina, 2011. http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA.

Nagyfejeo, Eva, and Sarah Puello Alfonso. “Cybersecurity Capacity Review Bosnia and Herzegovina.” *SSRN Electronic Journal*, 2019, 1–87. https://doi.org/10.2139/ssrn.3658404.

Newmeyer, Kevin P. “Elements of National Cybersecurity Strategies for Developing Nations.” *National Cybersecurity Institute Journal* 1, no. 3 (2015): 9–19. http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf#page=11.

Nišević, Maja, Chiara Zamboni, and Bojan Kovačević. "Cryptocurrencies: Highlighting the Perspective of Bosnia and Herzegovina." *International Review of Law, Computers & Technology*, December 2, 2021, 1–20. https://doi.org/10.1080/13600869.2021.2004759.

North Atlantic Treaty Organisation (NATO). "Relations with Bosnia and Herzegovina." NATO, 2021. https://www.nato.int/cps/en/natohq/topics_49127.htm.

Organisation for Security and Co-operation in Europe (OSCE). "BiH Ministry of Defence and OSCE Mission to BiH Organize 13th Strategic Political-Military Seminar on Cybersecurity and Crisis Management." www.osce.org, December 8, 2021. https://www.osce.org/mission-to-bosnia-and-herzegovina/507446.

———. "Cyber Security." Organisation for Security and Co-operation in Europe (OSCE). Accessed February 25, 2022. https://www.osce.org/files/f/documents/c/4/468369.pdf.

———. "Cyber-Attacks on Online Media Endanger Media Freedom in BiH." www.osce.org, 2021. https://www.osce.org/mission-to-bosnia-and-herzegovina/479621.

———. "Guidelines for a Strategic Cybersecurity Framework in Bosnia and Herzegovina." *Www.osce.org*. Organisation for Security and Co-operation in Europe (OSCE), 2019. https://www.osce.org/mission-to-bosnia-and-herzegovina/438383.

———. "The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Focus on South-Eastern Europe." Organization for Security and Co-operation in Europe (OSCE), 2018. https://polis.osce.org/role-civil-society-preventing-and-countering-violent-extremism-and-radicalization-lead-terrorism.

Organisation for Security and Co-operation in Europe Permanent Council. Osce Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (2016). https://www.osce.org/files/f/documents/d/a/227281.pdf.

Pawlak, Patryk. "Operational Guidance for the EUs International Cooperation on Cyber Capacity Building." Luxembourg: European Union Institute for Security Studies (EUISS), 2018. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf.

Personal Data Protection Agency in Bosnia and Herzegovina. "Competencies." www.azlp.ba. Accessed February 25, 2022. http://www.azlp.ba/o_agenciji/nadleznosti/default.aspx?id=459&langTag=en-US&template_id=149&pageIndex=1.

———. "Regulation (EU) 2016/679 of the European Parliament and of the Council." azlp.ba. Accessed February 25, 2022. http://azlp.ba/GDPR_Menu/Opsta_uredba/default.aspx?id=2366&langTag=en-US&template_id=149&pageIndex=1.

Presidenza del Consiglio dei Ministri. "DECRETO-LEGGE 14 Giugno 2021, N. 82 [Decree-Law 14th of June 2021, No. 82]." www.normattiva.it, 2021. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-14.

Prime Minister's Office. “Israel National Cyber Security Strategy in Brief,” 2017. https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

Public Safety Canada. *National Cyber Security Strategy : Canada’s Vision for Security and Prosperity in the Digital Age*. Ottawa, Ontario: Public Safety Canada, 2018.

Royal Canadian Mounted Police (RCMP). “Royal Canadian Mounted Police Cybercrime Strategy,” 2015. https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf.

Security and Intelligence Group (SIG). “National Plan to Address Cybercrime,” 2015. https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy.

Stojanovic, Milica, Bojan Stojkovski, Samir Kajosevic, Nermina Kuloglija, and Fatjona Mejdini. “Cyber-Attacks a Growing Threat to Unprepared Balkan States.” Balkan Insight, March 10, 2021. https://balkaninsight.com/2021/03/10/cyber-attacks-a-growing-threat-to-unprepared-balkan-states/.

Stojanović, Zvezdan, and Mehrudina Musić. “Development of E-Government in Bosnia and Herzegovina.” *Journal Human Research in Rehabilitation* 8, no. 1 (April 2018): 70–76. https://doi.org/10.21554/hrr.041810.

The Financial Action Task Force (FATF). “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.” The Financial Action Task Force (FATF), 2021. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

———. “Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.” The Financial Action Task Force (FATF), 2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

The Government of Japan. “Cybersecurity for All,” 2021. https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021-en-booklet.pdf.

The NATO Science for Peace and Security Programme. “Country Flyer 2021 Bosnia and Herzegovina,” 2021. https://www.nato.int/science/country-fliers/BIH.pdf.

The Soufan Center. “IntelBrief: Terrorists’ Use of Cryptocurrency.” *The Soufan Center* (blog), December 10, 2020. https://thesoufancenter.org/intelbrief-2020-december-10/.

The United States Agency for International Development (USAID). “Bosnia and Herzegovina. Country Development Cooperation Strategy (CDCS), December 2020 - December 2025.” The United States Agency for International Development (USAID), 2020. https://www.usaid.gov/sites/default/files/documents/BiH_CDCS_external_Dec_2025.pdf.

The White House. “National Cyber Strategy of the United States,” 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Turkish Cooperation and Coordination Agency (TİKA). “About Us - TİKA.” Tika.gov.tr, 2011. https://www.tika.gov.tr/en/page/about_us-14650.

United Nations Development Programme (UNDP). “Digital Transformation in Business.” Undp.org, 2022. https://open.undp.org/projects/00126505.

United Nations Development Programme (UNDP) in Bosnia and Herzegovina. “Digital Transformation in Business – DigitalBIZ | UNDP in Bosnia and Herzegovina.” United Nations Development Programme (UNDP) in Bosnia and Herzegovina, 2020. https://www.ba.undp.org/content/bosnia_and_herzegovina/en/home/development-impact/DigitalBiz.html.

Vakulyk, Olga, Pavlo Petrenko, Iulia Kuzmenko, Maksym Pochtovyi, and Ruslan Orlovskyi. “Cybersecurity as a Component of the National Security of the State.” *Journal of Security and Sustainability Issues* 9, no. 3 (March 25, 2020): 775–84. https://doi.org/10.9770/jssi.2020.9.3(4).

Vasiu, Ioana, and Lucian Vasiu. “Cybersecurity as an Essential Sustainable Economic Development Factor.” *European Journal of Sustainable Development* 7, no. 4 (October 1, 2018): 171–78. https://doi.org/10.14207/ejsd.2018.v7n4p171.

Wang, Shacheng, and Xixi Zhu. “Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing.” *Policing: A Journal of Policy and Practice* 15, no. 4 (September 7, 2021). https://doi.org/10.1093/police/paab059.

World Bank. “Individuals Using the Internet (% of Population) - Bosnia and Herzegovina | Data.” data.worldbank.org. Accessed February 28, 2022. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BA.

ANNEX A – Questionnaire provided to BiH public institutions

1. Is cybersecurity a top priority for your institution?

○ Yes
○ No

1.1. **To be completed only if the answer to question 1 is "Yes":** Does your institution have an internal document regulating cybersecurity issues?

○ Yes
○ No

2. Has your institution participated in courses, trainings or workshops to raise awareness and knowledge about cybersecurity in the period from 2019 to 2022?

○ Yes
○ No

2.1. **To be completed only if the answer to question 2 is "Yes":** How many of such events?

2.2. **To be completed only if the answer to question 2 is "Yes":** Please provide the name of the organizer of these events:

3. Can you list relevant government documents related to cybersecurity?

4. **Question provided ONLY for police officers / investigators:** How many cybercrime cases have you documented in the period from 2019 to 2021?

2019.	2020.	2021.

5. Can you name some trends that characterize cybercrime?

6. Can you list some international standards regarding cybersecurity?

7. Was your institution a victim of cyber-attacks in the period from 2019 to 2022?

○ Yes
○ No

8. How would you assess the cyber capabilities of your institution?

A. Excellent
B. Good
C. Average
D. Fair
E. Poor

9. In your opinion, how would you assess the awareness of BiH citizens about cybersecurity?

A. Excellent
B. Good
C. Average
D. Fair
E. Poor

ANNEX B – Definitions[111]

Cybersecurity

The ability to protect or defend the use of cyberspace from cyberattacks.

Cyberspace

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyberattack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber awareness

Knowledge end-users have about the cyber threats and risks their networks can face and about best practices to guide their behaviours.

Cyber threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Cyber risk

The risk of depending on cyber resources (i.e., the risk of depending on a system or system elements that exist in or intermittently have a presence in cyberspace).

Cybercrime

Any action by a state, group or criminal organisation facilitated by or using cyberspace targeting another state.

[111] The definitions are from the glossaries provided by the National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA). See: https://csrc.nist.gov/glossary; https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

ANNEX C – List of institutions that provided answers to the questionnaire

Bosnia and Herzegovina (BiH):
Directorate for Coordination of Police Bodies of Bosnia and Herzegovina
Ministry of Defence
Ministry of Security Agency for Education and Professional Training
Ministry of Security Agency for Forensic and Expert Examinations
Ministry of Security border police
Ministry of Security Police Support Agency
Ministry of Security State Investigation and Protection Agency

Federation of Bosnia and Herzegovina (FBiH):
Bosnian-Podrinje Canton Ministry of Interior
Central Bosnian Canton Ministry of Interior
Federal Police Administration
Judicial Police
Posavina Canton Ministry of Interior
Sarajevo Canton Ministry of Interior
Tuzla Canton Ministry of Interior
Una-Sana Canton Ministry of Interior
West Herzegovina Canton Ministry of Interior
Zenica-Doboj Canton Canton Ministry of Interior

Republic of Srpska (RS):
Ministry of the Interior of the Republic of Srpska

Brčko District (BD):
Police Brčko District

Centar za sigurnosne studije - BIH

Centre for Security Studies - BH

BOSNA I HERCEGOVINA
71000 SARAJEVO
BRANILACA SARAJEVA 13/1

TEL:
+ 387 (0)33 262-456

info(at)css.ba

@CSSBIH

www.css.ba