CYBERSECURITY CAPACITY REVIEW

Bosnia and Herzegovina

March 2019

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Dr Eva Nagyfejeo, Dr Sarah L Puello Alfonso

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Professor Basie Von Solms, Professor Federico Varese, Dr Jamie Saunders

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*18/12/2018*	*First draft submitted to Technical Board*
2	*25/1/2019*	*Second draft submitted to World Bank*
3	*27/1/2019*	*Second draft submitted to Ministry of Communications and Transport*
4	*22/3/2019*	*Third draft submitted to World Bank and Ministry of Communications and Transport*

LIST OF ABBREVIATIONS

AEPTM	Agency for Education and Professional Training
BAS	Institute for Standardization of Bosnia and Herzegovina
BD	Brčko District
BiH	Bosnia and Herzegovina
CBBH	Central Bank of Bosnia and Herzegovina
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEPOL	European Union Agency for Law Enforcement Training
CEO	Chief Executive Officer
CI	Critical infrastructure
CISSP	Certified Information Systems Security Professional
CISSP	Certified Information Systems Security Professional
CoE	Council of Europe
CRA	Communications Regulatory Agency
CSIRT	Computer Security Incident Response Team
EC3	European Cybercrime Centre
EU	European Union
EUROPOL	European Union Agency for Law Enforcement Cooperation
FBiH	Federation of Bosnia and Herzegovina
FRONTEX	European Border and Coast Guard Agency
GDPR	EU General Data Protection Regulation
HIDS	Network Introduction Detection Systems
IDDEEA	Agency for Identification Documents, Registers and Data Exchange
ISO	International Organization for Standardization
ISP	internet service provider
J-CAT	Joint Cybercrime Action Taskforce
MAP	Membership Action Plan
MLA	Mutual Legal Assistance
MoCA	Ministry of Civil Affairs of BiH
NATO	The North Atlantic Treaty Organization
NGO	non-governmental organisation
NIDS	Network Introduction Detection Systems
NIS	Directive on security of network and information systems

NSA	National Security Authority
OLAF	European Anti-Fraud Office
OSCE	Organization for Security and Co-operation in Europe
PPP	public–private partnership
QMS	quality management system
RS	Republic of Srpska
SIPA	State Investigation and Protection Agency
SSL	Secure Sockets Layer
TAIEX	Technical Assistance and Information Exchange
TLS	Transport Layer Security
VPN	Virtual Private Network

EXECUTIVE SUMMARY

In collaboration with the World Bank (WB), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in Bosnia and Herzegovina at the invitation of the Ministry of Communications and Transport. The objective of this review was to enable the Government to gain an understanding of its cybersecurity capacity in order to develop the country's national cybersecurity strategy, and to strategically prioritise investment in cybersecurity capacities.

Over the period 23–25 October 2018, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, defence community, information-technology officers and representatives from public-sector entities, critical-infrastructure owners, policy makers, information-technology officers from the private sector (including financial institutions), telecommunications companies, the banking sector as well as international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cyber Culture and Society*
- *Cybersecurity Education, Training and Skills*
- *Legal and Regulatory Frameworks*
- *Standards, Organisations, and Technologies*

Each dimension comprises *factors,* which describe what it means to possess cybersecurity capacity. Factors present a number of *aspects* which group together related *indicators*, which describe steps and actions that, once observed, define the stage of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in Bosnia and Herzegovina and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre and 'dynamic' is placed at the perimeter.

[1] Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (assessed 25 February 2018)

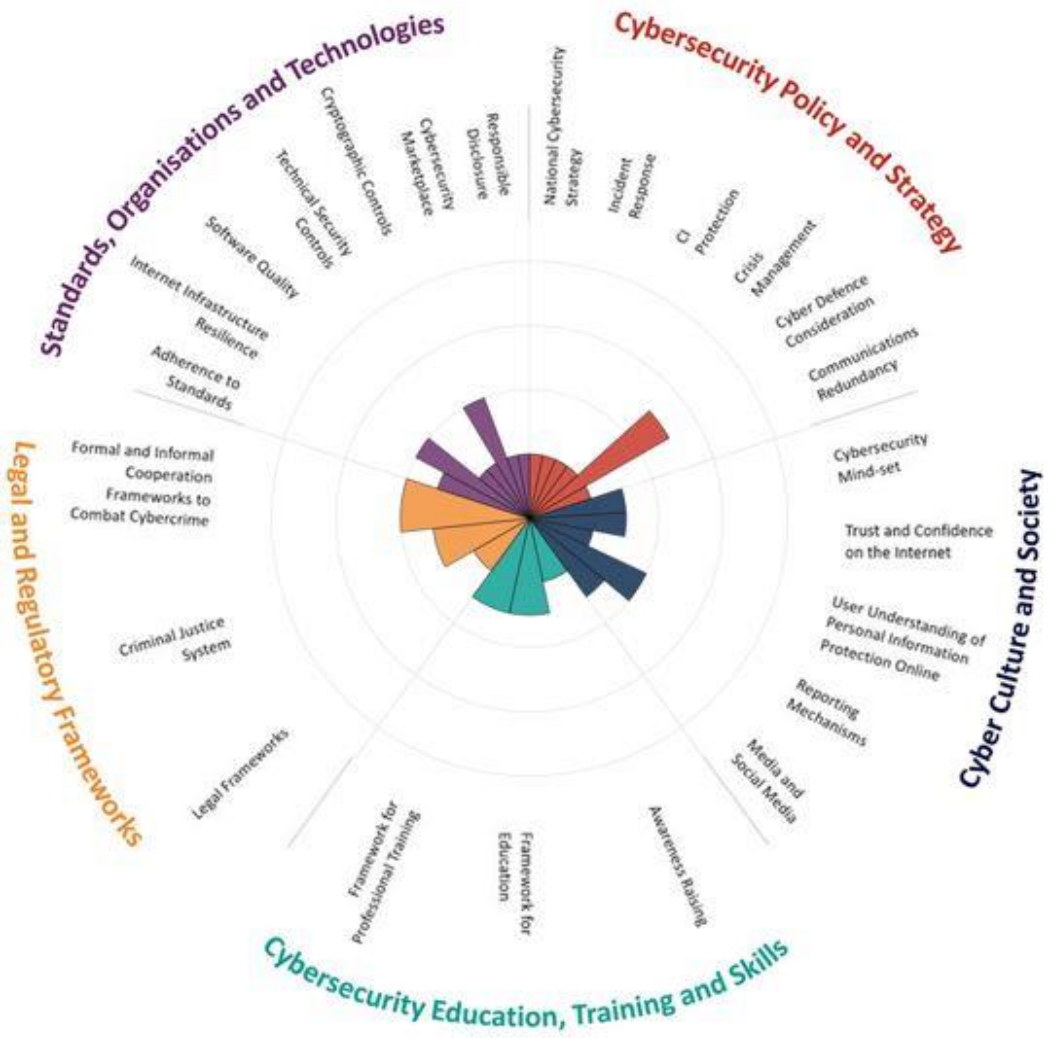

Figure 1: Overall representation of the cybersecurity capacity in Bosnia and Herzegovina

Cybersecurity Policy and Strategy

Currently, there is no official national cybersecurity document in Bosnia and Herzegovina (BiH) detailing how to establish coordination between key cybersecurity governmental and non-governmental actors nor is there an overarching national cybersecurity programme.

However, consultation processes for strategy development have been initiated where different actors are invited based on the development process. Statement from participants suggested that the Ministry of Security is leading the development of the strategy jointly with the Organization for Security and Co-operation in Europe (OSCE) who is assisting in organising, monitoring and implementing the process.

Currently, at the state level there is no registry or catalogue of national level incidents centrally managed by the government, nor is there a national coordinating body (such as Computer Security Incident Response Team (CSIRT, or CERT) in order to effectively coordinate cybersecurity incident response and management. Also, there is no mandatory reporting

requirements for cyber incidents. At the entity level, the first CERT was established (in 2015) with the creation of the Department for Information Security within the Agency for Information Society of the Republic of Srpska.[2]

The concept of cybersecurity in critical infrastructure (CI) is still in its infancy in BiH. At the state level, there is as yet no accepted definition of national CI and no formal categorisation of CI assets. Interaction between government ministries and owners of CI assets is limited and ad-hoc.

The extent to which organisations consider cyber threats as part of crisis situations is uncertain. Risk management exercises and cyber drills at the state level have not yet been formalised.

The Ministry of Defence has developed its own cyber defence strategy with the aim to establish a secure cyber environment for the information systems within its Ministry only. This strategy was developed without the adoption of an official national cybersecurity strategy. However, participants anticipate that the Ministry's strategy will help to improve the overall cyber security level within the country.

It was difficult to obtain a clear picture regarding communications redundancy during the review. Digital redundancy measures are considered (in an ad-hoc manner) by private telecommunication companies and other organisations, but there was no clear indication of systematic coordination at the state level. Participant commentary indicated that at the state level there have been no exercises or drills conducted to test emergency response under circumstances with disrupted communications.

Cyber Culture and Society

The cybersecurity mind-set in Bosnia and Herzegovina is still in an early, nascent state of development. Participants from both the public and private sectors described an overall low level of awareness of the values, attitudes and practices necessary for a healthy cybersecurity ecosystem. This lack of awareness is the result of limited knowledge of existing cyber threats, which in turn stems from a lack of harmonisation in the legislation, in established mechanisms for awareness-raising and most saliently in the challenge of designating a cohesive implementation lead for cyber issues in Bosnia and Herzegovina.[3]

The results of this assessment have shown dissenting views when it comes to users' overall trust and confidence in the internet. Some participants indicated that Bosnians are not trusting of the government, an attitude that also limits their ability to trust in the limited e-government services available. Bosnians feel insecure about the services available to them, which was remarked as most likely linked to an overall lack of awareness and understanding of the possible threats – lack of ICT literacy.

[2] Council of Europe (2017) Bosnia and Herzegovina. Octopus Cybercrime Community. Available at https://www.coe.int/en/web/octopus/countrywiki//asset_publisher/hFPA5fbKjyCJ/content/bosniaandherzegovina?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountrywiki%3Fp_p_id%3D101_INSTANCE_hFPA5fbKjyCJ%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1 (Accessed 7/11/2018)

[3] Baraković, S. and Jasmina Baraković Husić (2015). "'We have problems for solutions': The State of Cybersecurity in Bosnia and Herzegovina". *Information & Security: An International Journal, vol. 32* [online] Available at: http://dx.doi.org/10.11610/isij.3205 [Accessed 14 Nov. 2018], p.4.

E-commerce services are often offered in an unsecure environment. They are being provided to a limited extent and when they provided, a limited proportion of users trust in the secure use of e-commerce services.

In Bosnia and Herzegovina, Internet users and stakeholders within both the public and private sectors recognised that there is no systematic user understanding of personal information protection online. These participants remarked that only a small proportion of the population – and in most cases, these are people who already work in the cyberspace – practice caution when sharing information online or using online services. Most people share information in social networks with little discrimination, unaware of the degree to which sensitive personal information should be kept private.

The main reporting entity in Bosnia and Herzegovina, both at the entity and cantonal levels, is the police. Each of the two entities, the Federation of Bosnia and Herzegovina and Republic of Srpska has their own police force governed by the Directorate for Coordination of Police Bodies of Bosnia and Herzegovina. The reality remains that law enforcement in Bosnia and Herzegovina assumes most of the responsibility when addressing online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches and other incidents. This assessment did determine that the existing channels of reporting, particularly between entities and regions is not coordinated and is used in an ad-hoc manner.

In Bosnia and Herzegovina, cybersecurity issues are overall insufficiently reported across mainstream media both online and offline.

Cybersecurity Education, Training and Skills

Awareness of cybersecurity risks and threats in Bosnia and Herzegovina is still low at all levels of society, and our research identified that awareness of cybersecurity threats and vulnerabilities across all sectors is currently in the initial stages of discussion. Participants admitted that awareness raising is not a priority for government institutions, in part because there is a lack of knowledge around what possible risks and threats might exist.

Additionally, when present, awareness-raising programmes appear to still be informed by international initiatives, like the one revealed by one participant, which involves a proposal for a digital skills training campaign of a value of £10M coordinated in the Western Balkans by the British Council.

Awareness raising on cybersecurity issues for executives is limited, though more systematically present than in the wider population, particularly in the case of multinational or executives from the finance sector, which do have more specific guidelines to follow. For example, participants described that in the banking sector, workshops are delivered on a regular basis. In the majority of companies, executives are not yet always aware of their responsibilities to shareholders, clients, customers, and employees in relation to cybersecurity.

At primary and secondary levels of education, participants explained that cybersecurity-related topics include less than a year of lessons, concentrated on no more than one module within existing Information Technology courses. Some schools also provide programmes to teach educators and schoolchildren about safety on the internet; in some cases, this work is being done through non-governmental organisations (NGOs). The education is Bosnia and

Herzegovina is not offered at a state level, and therefore considerably fragmented, which inevitably affects consolidated provisions.

At the higher education level, computer science courses are offered that may have a security component, but no cybersecurity-related courses are offered. Some educational courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet available.

Bosnia and Herzegovina offers some cybersecurity training programmes to professionals working in different sectors, but this provision appears to be ad-hoc, and not readily recognised by the government.[4] This lack of recognition was pointed out as one of the factors behind the low number of cybersecurity-aware experts and the prevalence of software developers.

Legal and Regulatory Frameworks

Bosnia and Herzegovina (BiH) has an extremely complex system of government that is reflected in the existing legislation of the country. BiH is composed of the Federation of Bosnia and Herzegovina (FBiH), the Republic of Srpska (RS) and the Brčko District (BD), which are self-governing entities each with its own Criminal Code and Criminal Procedural Code that address offences related to cybercrime.[5]

At the state level, the Criminal Code and Criminal Procedural Code focus on tackling the most serious criminal offences such as organised crime and crimes against humanity. Issues related to cybersecurity and cybercrime are therefore dispersed under four Criminal Codes and Laws on Criminal Procedure (one at the state level and three at the entities' level).

Despite the fact that BiH signed the Budapest Convention in 2005 and ratified it in 2006 entering into force in the same year, the existing legislations at the state level are only partially harmonised and have not fully implemented the provisions of the Budapest Convention on Cybercrime.[6] Also, adopted or amended legislation does not cover all aspects of cybersecurity, such as human rights protection online and consumer protection and intellectual property online.

BiH has not adopted specific legislation on human rights online. According to the Human Rights Report provided by the U.S. Department of State for 2017 there was no violation of Internet freedom by the government.[7]

BiH has a very complex organizational criminal justice system, which is determined by a complex constitutional structure of the state. Participants' commentary indicated that institutional capacities to tackle cybercrime issues remain at the entity level. At the state level, there is no specialised cybercrime unit to combat cybercrime. The Directorate for

[4] ITU (2018). Readiness Assessment Report to Establish a CIRT Network in Bosnia and Herzegovina, p.24-25.
[5] Murtezic, A. (2014) Assessment of compliance of the criminal codes in Bosnia and Herzegovina with the council of Europe cybercrime convention. Available at http://krimteme.fkn.unsa.ba/index.php/kt/article/viewFile/169/pdf (Accessed 9/11/2018)
[6] DiploFoundation (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. Available at https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf (Accessed 9/11/2018)
[7] US Department of State. Bosnia and Herzegovina 2017 Human Rights Report. Available at https://www.state.gov/documents/organization/277391.pdf (Accessed 14/11/2018)

Coordination of Police Bodies of BiH within the Ministry of Security only fulfils a coordinating role and manages inter-entity requests.[8]

At the state level, it was not possible to obtain a clear picture regarding the capacity of law enforcement, prosecutors and judges, however participant comments suggested that the judiciary, prosecutors and the police do not have adequate knowledge and skills to investigate cybercrime cases. At the state level, the Agency for Education and Professional Training (AEPTM), established in 2009, is in charge of 'providing research and education in the field of police education and security'.[9]

The working-level cooperation between the judiciary, law enforcement, government and private sector was described by participants as informal and poor due to the different degrees of cooperation that exist between the law enforcement agencies. At the state level, the Ministry of Security and European Union Agency for Law Enforcement Training (CEPOL) entered into a working agreement in 2014 in order to enhance mutual cooperation on law enforcement training.[10] There is a designated point of contact for maintaining communication including the Ministry of Security, the Ministry of the Internal Affairs of the Republic of Srpska, and the Ministry of the Interior of the Federation of BiH.[11]

Standards, Organisations, and Technologies

The Law on Standardization of Bosnia and Herzegovina and the Law on the Establishment of the Institute for Standardization of Bosnia and Herzegovina have laid the foundation for promoting the voluntary implementation and use of BiH national standards, compliance with the rules of international and European standardization and the creation of the Institute for Standardization that acts as an independent state administrative organization for the activities in the field of standardization. The review found that participants from both the public and private sectors were not aware of any ICT standards promoted by the government.

Similarly, at the state level there is no mandatory standard for any sector related to the procurement of hardware and software. Focusing on standards in software development, different guidelines exist in both the public and the private sectors, but the extent to which these guidelines are related to cybersecurity is not clear.

The economic prosperity, including the further liberalization of the telecommunications market and the introduction of new technologies for broadband internet, largely depends on the country's continuing integration with the EU. Bosnia and Herzegovina's Communications Regulatory Agency (CRA) published a Report on users of CRA licenses for the provision of internet services in BiH for 2017. According to Communications Regulatory Agency (CRA), the broadband internet penetration subscriber base in Bosnia and Herzegovina reached 663,682

[8] Council of Europe (2017) iPROCEEDS. General guide on Protocols on interagency and international cooperation for investigations involving proceeds from crime online. Available at https://www.coe.int/en/web/cybercrime/iproceeds (Accessed 9/11/2018)
[9] Agency for Education and Professional Training. https://www.aeptm.gov.ba/en/node/300 (Accessed 9/11/2018)
[10] CEPOL (2014) CEPOL signs Working Arrangement with Bosnia and Herzegovina. Available at https://www.cepol.europa.eu/media/news/cepol-signs-working-arrangement-bosnia-herzegovina (Accessed 14/11/2018)
[11] Council of Europe. Octopus Cybercrime Community (2017) Bosnia and Herzegovina. Available at https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/bosnia-and-herzegovina?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view (Accessed 9/11/2018)

individuals as of 2017, thus translating to around 19% of broadband access in the country (the number of connections in relation to the total number of inhabitants).[12]

Based on the review, there is no identified centrally managed catalogue of secure software platforms and applications at the state level in BiH. Policies for updating software products or monitoring the functionality of applications may exist but are not necessarily enforced or formulated – each organisation has its own requirements defined at the corporate level.

The adoption of technical security controls in the country varies across the sectors within the entities and organisations, but they are mostly ad hoc and not consistently deployed.

At the state level, cryptographic controls (SSL, VPN) for protecting data at rest and in transit are recognised and deployed ad hoc by multiple stakeholders and within various sectors.

Participants from the public and private sectors noted that BiH does not currently produce cybersecurity technologies, but relies on international offerings. Currently, there is no policy in place for responsible information disclosure within the public or the private sectors.

Within public institutions, training on cybersecurity issues both for IT and general staff is limited and often takes place through the incentive of the respective management in the institution. At the State level, initiatives exist; but these rely on individual institutions expressing the need for adequate training, and for it to be then carried out. The trainings offered can vary between general cybersecurity training and certified courses, but resources still appear to lack.

Additional Reflections

Even though the duration of this review was shorter by half a day, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 28th country review that the GCSCC have supported directly.

[12] Communications Regulatory Agency. https://docs.rak.ba//documents/d4a46a61-18f8-45b2-afc5-b1784f009fe8.pdf

INTRODUCTION

In collaboration with the World Bank (WB), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in Bosnia and Herzegovina at the invitation of the Ministry of Communications and Transport. The objective of this review was to enable the Government to gain an understanding of its cybersecurity capacity in order to develop the country's national cybersecurity strategy, and to strategically prioritise investment in cybersecurity capacities.

Over the period 23–25 October 2018, the following stakeholders participated in roundtable consultations:

- Public sector entities
  - Parliament BiH - Information Technology Sector
  - Ministry of Civil Affairs of Bosnia and Herzegovina – Sector for Education
  - Ministry of Finance / Finance and Treasury of Bosnia and Herzegovina
  - Ministry of Foreign Affairs of Bosnia and Herzegovina
  - Ministry of Communications and Transport of Bosnia and Herzegovina
  - Ministry of Foreign Trade and Economic Relations of Bosnia and Herzegovina
  - Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina
  - The Information Society Agency of Republika Srpska
  - Ministry of Defence of Bosnia and Herzegovina
  - Ministry of Security of Bosnia and Herzegovina
  - Ministry of Communications and Transport of Bosnia and Herzegovina
  - Department for maintenance and development of electronic business and e-government system - General Secretariat of the Council of Ministers of BiH

- Criminal justice sector
  - Ministry of Security of Bosnia and Herzegovina
  - Federal Police Administration
  - Ministry of the Interior of Republika Srpska
  - Ministry of Justice of Bosnia and Herzegovina
  - The Prosecutor's Office of Bosnia and Herzegovina

- Finance sector
  - BIT alianseAlliance
  - ICT Association of Foreign Trade Chamber of Bosnia and Herzegovina
  - BH Telecom
  - Eronet
  - Mtel
  - Central Bank of Bosnia and Herzegovina

- Critical infrastructure owners
  - Communications Regulatory Agency of Bosnia and Herzegovina
  - Elektroprenos BiH

- The State Electricity Regulatory Commission of Bosnia and Herzegovina

- National Security Agencies
  - Ministry of Defence of Bosnia and Herzegovina
  - Intelligence – Security Agency of Bosnia and Herzegovina
  - Directorate for Coordination of Police Bodies of Bosnia and Herzegovina
  - Ministry of Security of Bosnia and Herzegovina

- Academia
  - University of Sarajevo
  - University of Mostar
  - University Tel-Informatic Centre - UTIC

- International community
  - OSCE

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM)[13] which is composed of five distinct *dimensions* of cybersecurity capacity.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions together with the factors which each presents:

DIMENSIONS	FACTORS
Dimension 1 Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 Cyber Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 Cybersecurity Education, Training and Skills	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 Legal and Regulatory Frameworks	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat CybercrimeCybercrime
Dimension 5	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality

[13] See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

Standards, Organisations, and Technologies	D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors present a number of aspects which group together related indicators, which in turn describe steps and actions that once observed define which stage of maturity this aspect is at. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **Start-up:** at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.
- **Formative:** some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new However, evidence of this aspect can be clearly demonstrated.
- **Established:** the indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.
- **Strategic:** at this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the particular circumstances of the state or organisation.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Bosnia and

Herzegovina and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Bosnia and Herzegovina and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

METHODOLOGY - MEASURING MATURITY

During the country review specific dimensions are discussed with the relevant group of stakeholders. Each stakeholder cluster is expected to respond to one or two dimensions of the CMM, depending on their expertise. For example Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 and Dimension 3 of the CMM.

In order to determine the level of maturity, each aspect has a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions stakeholders should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[14] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[15] It is this interaction and tension that offers advantage over other

[14] Relevant publications:
Williams, M. (2003).Making sense of social research. London: Sage Publications Ltd. doi: 10.4135/9781849209434
Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. SAGE Focus Editions: Successful focus groups: Advancing the state of the art (pp. 35-50). Thousand Oaks, CA: SAGE Publications Ltd. doi: 10.4135/9781483349008
Krueger, R.A. and Casey, M.A. (2009). Focus groups: A practical guide for applied research. London: Sage Publications LTD.

[15] Relevant publications: J. Kitzinger. 'The methodology of focus groups: the importance of interaction between research participants.' Sociology of Health & Illness, 16(1):103–121, 1994.
J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299– 302, 1995.
E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, pages 1–13, 1982.

methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[16]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to the data generated by focus groups.[17] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[18]

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[19] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[20] Dey explains that this process categorises data as "belonging together".[21]

The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.[4]

In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a third, blended approach in the analysis of our data, which is a mixture of deductive and inductive approaches.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and use the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

---

[16] J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299– 302, 1995.

[17] K. Krippendorff. Content analysis: An introduction to its methodology. Sage Publications, Inc, 2004. H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.
K.A. Neuendorf. The content analysis guidebook. Sage Publications, Inc, 2002.

[18] E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, Volume and Number? pages 1–13, 1982.

[19] S. Elo and H. Kyng¨as. 'The qualitative content analysis process.' Journal of Advanced Nursing, 62(1):107–115, 2008.
H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.

[20] P.D. Barbara Downe-Wamboldt RN. 'Content analysis: method, applications, and issues.' Health Care for Women International, 13(3):313–321, 1992.

[21] I. Dey. Qualitative data analysis: A user-friendly guide for social scientists. London: Routledge, 1993.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders.

Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of Bosnia and Herzegovina and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN BOSNIA AND HERZEGOVINA

Bosnia and Herzegovina (BiH) has an extremely complex system of governance, composed of the Federation of Bosnia and Herzegovina (FBiH), the Republic of Srpska (RS) and the Brčko District (BD). Throughout the report 'state level' indicates the whole area of the country/nation, whilst 'entity level' refers to FBiH and RS as self-governing entities and to BD as Brcko District (or Government of Brcko District) that is a self-governing district.[22] The complex and decentralised structure of the country poses a challenge to progress in the field of cybersecurity and to reach consensus among the different stakeholders.

Figure 1: Territorial organization of Bosnia and Herzegovina[23]

[22] World Bank (2015) Country Partnership Framework For Bosnia And Herzegovina For The Period Fy16-Fy20. http://pubdocs.worldbank.org/en/215221450204091066/WBG-Bosnia-and-Herzegovina-period-FY2016-2020.pdf

[23] Ibid.

BiH has a resident population of approximately 3,856,181.[24] According to Bosnia and Herzegovina's Communications Regulatory Agency (CRA) in 2015 there were 2,782,107 Internet users, estimating that the Internet penetration rate was 72.41% in BiH.[25] In 2017, based on the CRA's survey results the number of individuals using the Internet increased to 3,064,072, estimating the internet penetration rate was 86.77%.[26] Such increases in adoption has led BiH being ranked 83th on the International Telecommunications Union (ITU) Global ICT Development Index ranking, which indicated that in 2017 there were 17.37 % fixed (wired)-broadband subscriptions per 100 inhabitants, compared to 37.35 % active mobile-broadband subscriptions per 100 inhabitants.[27] Based on the World Economic Forum's Global Information Technology report, BiH ranks 32nd in the world on Affordability (including the cost of accessing ICT, either via mobile telephony or fixed broadband Internet, as well as the level of competition in the Internet and telephony sectors that determine this cost).[28] Also, according to the 2017 Global Cybersecurity Index (GCI) published by the ITU, BiH ranks 135th in the world. [29]

A report published by DiploFoundation (2016) found that at the state level, a significant number of provisions on the Convention on Cybercrime are yet to be implemented.[30] Furthermore, currently, BiH does not have a strategic framework to address the issue of cybercrime and cyber security threats.[31] A working document published by the European Commission recognised that investigations in cybercrime (for e.g.: online child sexual abuse) remain extremely rare.[32]

In BiH, frameworks in cybersecurity education vary depending on the sector that is being addressed (primary to higher education) but also in the region of the country that is being focused on. The education sector in Bosnia and Herzegovina reflects the state constitution. It is defined by the BiH Constitution, the constitutions of the entities, cantons, and the Statute of Brčko District of BiH, which govern legal competencies in education. BiH consists of two entities (The Republic of Srpska and Federation of BiH) and Brcko district of BiH. The Republic of Srpska has a centralized government and one Ministry of Education. Federation of BiH has a decentralized government and consists of ten cantons where each canton has their own Ministry of Education. There is also Federal ministry of Education, but this ministry only has a coordinating role. In addition, Brcko district of BiH has a government with departments, with one of those department being the Department for Education. In accordance with that there

[24] CIA. World Factbook. Bosnia and Herzegovina. Available at https://www.cia.gov/library/publications/the-world-factbook/geos/bk.html (Accessed 16/12/2018)
[25] Communications Regulatory Agency (2015) Available at https://www.rak.ba/news/500 (Accessed 16/12/2018)
[26] Communications Regulatory Agency (2017) Available at https://www.rak.ba/news/569 (Accessed 16/12/2018)
[27] (ITU) Global ICT Development Index (2017) Available at https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&BIH (Accessed 16/12/2018)
[28] World Economic Forum (2016) The Global Information Technology Report 2016. Available at http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf (Accessed 16/12/2018).
[29] ITU (2017) Global Cybersecurity Index. Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (Accessed 16/12/2018)
[30] DiploFoundation (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities.
[31] European Commission (2018) Bosnia and Herzegovina 2018 Report. Available at https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-bosnia-and-herzegovina-report.pdf (Accessed 16/12/2018)
[32] Ibid.

are twelve responsible institutions of education in BiH. These include the Ministry of Education and Culture of the Republic of Srpska, ten cantonal ministries of education in the Federation of BiH and the Department for Education of the Brčko District of BiH Government. There are also two others ministries with a coordinating role. The Federal Ministry of Education and Science coordinates, among other things, activities within the Federation of BiH, between ten cantons. The Ministry of Civil Affairs of BiH (MoCA), established on a state level, coordinates activities within all education institutions in BiH. In accordance to the law, MoCA is responsible for carrying out activities and tasks within the jurisdiction of BiH related to defining basic principles of coordination of activities, harmonization of plans of entity bodies and defining strategy at the international level, including, among others, education. This is the body that would coordinate any initiatives related to cybersecurity education.

BiH has been an aspiring member of the North Atlantic Treaty Organization (NATO) and was invited to join the Membership Action Plan (MAP) in 2010.[33] Accession of BiH to the European Union remains the main foreign policy objective of the country. The country's accession would have significant cybersecurity implications, such as adhering to the General Data Protection Regulation and the NIS Directive that are both pre-requisites to boosting the European Digital Single Market.[34]

[33] NATO. Relations with Bosnia and Herzegovina. Available at https://www.nato.int/cps/en/natohq/topics_49127.htm (Accessed 16/12/2018)
[34] European Commission. Digital single market. Available at https://ec.europa.eu/commission/priorities/digital-single-market_en (Accessed 16/12/2018)

REVIEW REPORT

OVERVIEW

In this section, we provide an overall representation of the cybersecurity capacity in Bosnia and Herzegovina. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre and 'dynamic' at the perimeter.

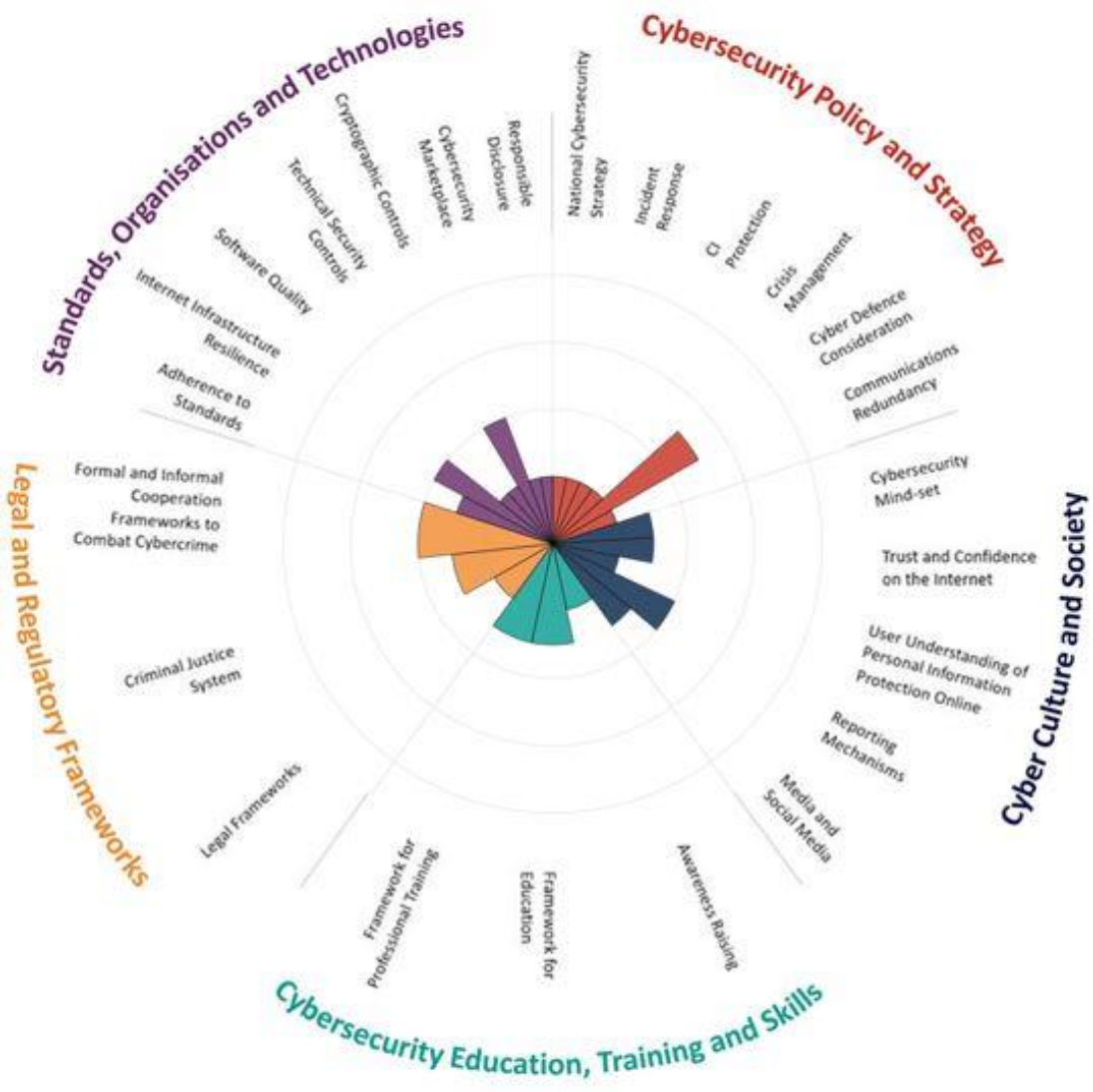

Figure 2: Overall representation of the cybersecurity capacity in Bosnia and Herzegovina

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

The factors in Dimension 1 gauge Bosnia and Herzegovina's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The Cybersecurity policy and strategy dimension also includes considerations for early warning, deterrence, defence and recovery. This dimension considers effective policy in advancing national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace increasingly vital for government, international business and society in general.

D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government, because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

Stage: Start-up

Currently, there is no official national cybersecurity document in Bosnia and Herzegovina (BiH) detailing how to establish coordination between key cybersecurity governmental and non-governmental actors nor is there an overarching national cybersecurity programme.

However, consultation processes for strategy development have been initiated where different actors are invited based on the development process. It was confirmed that the consultation involves all national security agencies (Ministry of Defence, Ministry of Security, Intelligence-Security Agency of BiH, Directorate for Coordination of Police Bodies of BiH), the Ministry of Communications and Transport, other regulatory bodies, the energy sector (joined recently), and one representative from the academic community, but excluding the private sector. The need to cooperate with the private sector will be highlighted in the upcoming strategy.

Statement from participants suggested that the Ministry of Security is leading the development of the Strategic Cyber Security Framework in Bosnia and Herzegovina jointly

with the OSCE who is assisting in organising, monitoring and implementing the process. It was not possible to obtain a clear picture regarding the content of the upcoming cybersecurity strategy however one participant indicated that the recommendations of the strategy will be based on the EU Directive on security of network and information systems (the NIS Directive) and ENISA's guidelines.[35] One participant referred to ENISA's National Cyber Security Strategy Good Practice Guide,[36] which helps to develop and update national cyber security strategies and based on that BiH focuses on nine objectives: 1) establishment of legal framework; 2) defining critical infrastructure; 3) protection of critical information infrastructure; 4) raising user awareness through education; 5) strengthening of trainings for the judiciary; 6) establishing an incident response capacity; 7) establishing incident reporting mechanisms; 8) establishing public-private partnerships (PPPs); 9) developing an Action Plan for the implementation of the strategy.

It was acknowledged during the review that there was no appropriate risk assessment conducted at the state level for the development of the cybersecurity strategy. However, once the strategy is published, it is intended to be a living document that will be revised and evaluated regularly.

Despite the fact that BiH lacks an official cybersecurity strategy, the Ministry of Security of Bosnia and Herzegovina has passed several documents that address cybersecurity, which were also adopted by the Council of Ministers of Bosnia and Herzegovina:

- the Strategy for Establishment of CERT in Bosnia and Herzegovina[37] (2011) - the first document at the state level addressing explicitly cybersecurity issues
- the Strategy for fight against organized crime in Bosnia and Herzegovina[38] (2017-2020)
- the Strategy on Combating Terrorism[39] (2015-2020)

Based on desk research, after the adoption of the Strategy for Establishment of CERT in 2011, an Expert Working Group was formed by the Council of Ministers for the establishment of BiH-CERT.[40] The Expert Working Group has completed its work regarding the implementation of the Strategy for Establishment of CERT, and a report along with a set of documents suggesting the way of establishing BiH-CERT has been adopted by the Council of Ministers of BiH. In this context, under the framework for cooperation with NATO, activities on preparing the application for the NATO Science for Peace and Security (SPS) Programme have been initiated, which should be realized in the medium term (3-5 years).

An Action Plan was also drafted by the Expert Working Group, which proposed the creation of a coordinating body by the Council of Ministers with the primary task to 'mitigate existing

[35] The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Available at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Accessed 7/11/2018)
[36] ENISA (2012) National Cyber Security Strategy Good Practice Guide. Available at https://www.enisa.europa.eu/publications/ncss-good-practice-guide (Accessed 8/11/2018)
[37] Ministry of Security (2011) Strategy for Establishment of CERT in Bosnia and Herzegovina. Available at http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=en-US (Accessed 7/11/2018)
[38] Ministry of Security (2017) Strategy for fight against organized crime in Bosnia and Herzegovina. Available at http://www.msb.gov.ba/PDF/strategy11122017.pdf (Accessed 7/11/2018)
[39] Ministry of Security (2015) Strategy on Combating Terrorism. Available at http://www.msb.gov.ba/PDF/STRATEGIJA_ZA_BORBU_PROTIV_TERORIZMA_ENG.pdf (Accessed 7/11/2018)
[40] Barakovic, S., & Husic, J. B. (2015) ''We Have Problems For Solutions'': The State Of Cybersecurity In Bosnia and Herzegovina. Information & Security, 32(2), 1. (Accessed 9/11/2018)

cybersecurity related problems through mandatory recommendations and support the process of establishing BiH-CERT and other CERTs in the country.'[41] However, the Action Plan was not adopted due to 'opposite political interests and stances' within the country that also hindered the institutional establishment of the BiH-CERT at the state level.[42]

At the entity level, the Government of the Republic of Srpska (RS) appointed an inter-departmental working group for drafting the Republic of Srpska Cyber Security Strategy (Decision No. 04/1-012-2-2322/16) and the Strategy for fight against cybercrime, however it has not been adopted yet.[43] In 2016, the 90th session of the Government of the Republic of Srpska concluded to disregard the proposal of forming a Working Group within the BiH Ministry of Security for the coordination of activities in the area of cybersecurity in BiH and regarded it unconstitutional.[44] According to the Government of RS, cybersecurity falls under the exclusive jurisdiction of the entity and 'a Working Group would transfer competences from the entity to the state level.'[45]

At the entity level, concerning the Federation of Bosnia and Herzegovina (FBiH), there are certain representatives from the Government of FBiH who are participating in the work of the Working Group within the BiH Ministry of Security responsible for the coordination of activities in the area of cybersecurity in BiH.

D 1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Start-up

Currently, at the state level there is no registry or catalogue of national level incidents centrally managed by the government, nor is there a national coordinating body (such as CSIRT or CERT) in order to effectively coordinate cybersecurity incident response and management. Also, there is no mandatory reporting requirements for cyber incidents.

Comments from focus-group participants suggested that incident-response efforts are not currently being coordinated across organisations. While some participants described steps that they took to handle incidents, the extent to which leads for incident response have been

[41] Ibid.
[42] Ibid.
[43] Council of Europe (2017) Bosnia and Herzegovina. Octopus Cybercrime Community. Available at https://www.coe.int/en/web/octopus/countrywiki//asset_publisher/hFPA5fbKjyCJ/content/bosniaandherzegovina?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountrywiki%3Fp_p_id%3D101_INSTANCE_hFPA5fbKjyCJ%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1 (Accessed 7/11/2018)
[44] Government of the Republic of Srpska (2016) The 90th session of the Government held. Available at http://www.vladars.net/eng/vlada/ic/ns/Pages/The-90th-session-of-the-Government-held--.aspx (Accessed 20/03/2019)
[45] Ibid.

formally designated within organisations is unclear. To illustrate, regarding the mechanisms of incident reporting, some participants mentioned that the Directorate for Coordination of Police Bodies only mediates and forwards the information received through international channels (such as INTERPOL) to the relevant agency in charge for the specific area. It was added that whilst the coordination responsibilities remain at the state level, the operational responsibilities remain at the entity level (Federation of Bosnia and Herzegovina and the Republic of Srpska).

At the entity level, the first CERT was established (in 2015) with the creation of the Department for Information Security within the Agency for Information Society of the Republic of Srpska.[46] It was added that a working group is supervising the CERT that is 'primarily tasked with coordination, prevention, and protection from incidents, as well as supervision of the implementation of measures and standards related to information security in the Republic of Srpska.'[47] One participant noted that information is discussed unofficially within the working group, and that the cooperation network and pre-agreed communication depends on personal connections and on the enthusiasm of the staff.

At the entity level, computer security incidents are reported either to the local police or to the Ministry of Interior of Republic of Srpska (handled by the Unit for Preventing High-tech Crime) that works closely with the Department for Information Security within the Agency for Information Society. As in the Republic of Srpska, the handling of computer security incidents is similar in the Federation of Bosnia and Herzegovina (FBiH). Based on desk research, incidents are handled by the Crime Police Department of the Federal Police Administration since there is no specialised cybercrime unit.[48] Usually, the Ministries of the Interior at the cantonal level and the Federal Ministry of Interior report computer security incidents to the Crime Police Department of the Federal Police Administration. Also, occasionally, citizens and companies report incidents directly to the Federal Police Administration. However, a large number of incidents are not reported, and companies manage incidents on their own in accordance with their internal security policies.

As no coordinating national incident-response organisation was yet established at the time this study was conducted, the associated roles, responsibilities and lines of communication or platforms required for broad collaboration on issues were not yet established.

In March 2017, the Council of Ministers adopted a decision on the establishment of a Computer Emergency Response Team and placing it under the aegis of the Ministry of Security, however there has not yet been the necessary political agreement to establish the BiH-CERT.

[46] Ibid.
[47] Ibid.
[48] Barakovic, S., & Husic, J. B. (2015) ''We Have Problems For Solutions": The State Of Cybersecurity In Bosnia and Herzegovina. Information & Security, 32(2), 1. (Accessed 9/11/2018)

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

Stage: Start-up

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

The concept of cybersecurity in critical infrastructure (CI) is still in its infancy in BiH. At the state level, there is as yet no accepted definition of national CI and no formal categorisation of CI assets. Interaction between government ministries and owners of CI assets is limited and ad-hoc.

It was difficult to establish the extent to which cybersecurity requirements and vulnerabilities in CI supply chains have been identified, mapped and managed; or the extent to which trust has been established between the government and CI organisations on the exchange of threat information.

D 1.4 CRISIS MANAGEMENT

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Start-up

The extent to which organisations consider cyber threats as part of crisis situations is uncertain. It is understood that general crisis management is necessary for national security, however, there is no evidence of any cybersecurity dimension to national crisis management and participants were unaware of any crisis management plan that involves coordination on national cybersecurity incidents. Risk management exercises and cyber drills at the state level have not been formalised yet.

D 1.5 CYBER DEFENCE

Stage: Formative – Established

This factor explores whether the government has the capacity to design and implement a cyber Defence strategy and lead its implementation, including through a designated cyber Defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

The Ministry of Defence (MoD) has developed its own cyber defence strategy with the aim to establish a secure cyber environment for the information systems within its Ministry only. This strategy was developed without the adoption of an official national cybersecurity strategy. However, participants anticipate that the Ministry's strategy will help to improve the overall cyber security level within the country.

During the review, it was not clear to what extent cyber operations units are incorporated into the different branches of the armed forces. At the time this study was conducted, there was no central cyber command or control structure at the state level.

It was confirmed by the participants that the two cybersecurity strategies (national and MoD's) will be coherent and harmonised, however there are still unfinished plans. The MoD's intention is to communicate requirements with all partners in a formal way. There might be a need to agree on memoranda of understanding (MOUs) with regards to information-sharing requirements, procedures and after that to establish technical capacities.

The MoD's strategy was described by participants as a general document that focuses on four main areas: 1) prevention of national security incidents; 2) response to incidents; 3) education and 4) awareness raising with end-users.

Before the final version of the strategy was adopted, participants highlighted that the Ministry held several events where participants from other institutions were invited such as the Ministry of Security. Furthermore, several international events were organised under the auspices of NATO. The final version of the strategy – that is quite general – is based on the Ministry's knowledge and the lessons learnt from these events. One participant acknowledged that the Ministry had to include some elements (guidelines and principles) that were supposed to be included in the national cybersecurity strategy. The goal is that these guidelines will be inter-operational with the national cybersecurity strategy at the state level.

The Ministry's strategy has recognised the importance of collaboration and information-sharing within the defence system concerning cyber-attacks. Therefore, the Ministry's CSIRT will be acting as one of the key points through which the Ministry will exchange information on cybersecurity related issues with both domestic and international stakeholders such as NATO.

Also, the Ministry of Defence developed an action plan to implement the strategy in the next five years and nominated a steering committee to oversee the implementation of the measures identified in the strategy. One of the key measures will be to establish a single

centre, which will be the main premise for the operational work of the CSIRT. If the Ministry succeeds in establishing the centre, then it will provide a cybersecurity situation room that will help in the management of cyber related incidents. This centre will likely be part of the command and control centre of the defence forces.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Start-up

It was difficult to obtain a clear picture regarding communications redundancy during the review. Digital redundancy measures are considered (in an ad-hoc manner) by private telecommunication companies and other organisations, but there is nothing coordinated and systematic at the state level.

Participant commentary indicated that at the state level there have been no exercises or drills conducted to test emergency response under circumstances with disrupted communications.

Focus groups discussions suggest that communications redundancy for emergency assets should be assured via phones and radio systems (back-up mechanisms for communications) that need to be part of contingency planning measures.

Participants agreed that each organisation should have an emergency response plan in place in order to ensure the continuity of the operation that deals most primarily with the communications aspect. One participant noted that the MoD has a contingency plan in place, however this plan should be part of a general plan of how the ministry should respond in case of emergency.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the government of BiH. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 Ensure that work towards developing a national cybersecurity strategy is progressed and that multi-stakeholder processes are followed consistently during the development processes of the strategy.

R1.2 Identify and involve key stakeholder groups, including international partners, and, at minimum, the organisations which participated in the CMM review.

R1.3 Expand the key stakeholder group, which is involved in the development of the national cybersecurity strategy, to include the financial sector, the private sector (including SMEs) that might be considered part of CI in the near future, as well as international partners.

R1.4 Establish a regular cycle for re-evaluating and updating the upcoming national cybersecurity strategy in response to recognised developments (e.g. every six months) and changes in the risk environment. Situation awareness over this environment should be supported by intelligence from international partners, reports from security analysts within organisations in BiH, and reports by security analysts who have been tasked by the government with monitoring developments in BiH and in the world at large.

R1.5 Allocate budget to ensure the development and implementation of cybersecurity strategic plans. Consider including international best practices (e.g. NIS and EU General Data Protection Regulation (GDPR) Directives).

R1.6 Design a methodology to analyse the results of the national cyber risk-assessment and incorporate lessons from this exercise in the development of the strategy.

R1.7 Consider developing a coordinated cybersecurity risk-analyst capacity. Cybersecurity risk-analyst skills are required for monitoring operations and developments in the risk environment (within specific organisations as well as within the world at large). These analysts should be able to bring together available data and information from various sources, such as system and user logs, reports from staff, news sources, service providers, and domestic and international partners, to create “risk profiles” specific for their organisational contexts. Ideally, every organisation that has a computer network should have someone with these skills, and cybersecurity management decisions should take into account findings from these analyses. A basic 12-step process for

intelligence-driven information security risk management is summarised at the end of the discussion section in Webb, Ahmad, Maynard and Shanks (2014).[49]

R1.8 Consider scenario and real-time cyber exercises to achieve a concurrent picture of national cyber resilience.

INCIDENT RESPONSE

R1.9 A mechanism for mandatory reporting of cybersecurity incidents needs to be established, which all organisations considered key to national security are expected to use. Information on reported incidents needs to be logged into a secure registry upon receipt, according to a standardised format, by qualified personnel who are charged with maintaining this registry.

R1.10 The government of BiH should work to ensure that there are qualified information- and cybersecurity professionals embedded in all organisations considered key to the national interest, and that each organisation has a designated lead for incident response.

R1.11 Establish the national CERT (BiH-CERT) under the auspices of the Ministry of Security of BiH at the state level. Once established, ensure that the national CERT has the necessary financial and human resources to fulfil its existing mandate for a national cyber incident response with clear processes and defined roles and responsibilities. Then consider establishing metrics to monitor and evaluate the effectiveness of BiH-CERT. The BiH-CERT should facilitate coordination between incident response personnel and international partners in emergency situations that meet agreed upon criteria.

R1.12 The government of BiH should endorse the adoption of specific standards and guidance related to incident management, to include monitoring requirements, performance metrics, reporting requirements, and minimum performance standards by all organisations considered key to the national interest.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.13 Develop and conduct a national risk assessment aiming to identify CI assets at the state level.

[49] Webb, J., Ahmad, A., Maynard, S.B. and Shanks, G., 2014. A situation awareness model for information security risk management. Computers & security, 44, pp.1-15, viewed 24 May 2018.

R1.14 Perform regular, detailed audits of CI assets with regards to cybersecurity and disseminate CI asset audit lists to relevant stakeholders. Inform CI stakeholders of their responsibilities.

R1.15 Establish a mechanism for regular vulnerability disclosure and information sharing between CI asset owners and the government. Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CI operators.

R1.16 Identify internal and external CI communication strategies with clear points of contact.

R1.17 Establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an incident response plan for cyber incidents.

R1.18 Establish common processes to measure and assess the capability of CI asset owners to detect, identify, respond to and recover from cyber threats.

CRISIS MANAGEMENT

R1.19 Designate an authority responsible for designing, planning and executing cybersecurity crisis management exercises at the state level.

R1.20 The cybersecurity crisis management authority should draw on the knowledge and expertise of stakeholders such as critical infrastructure asset owners; core business process owners and cybersecurity practitioners from other key organisations in BiH; academics; civil leaders and consultants.

R1.21 Exercise designs should be based on realistic incident scenarios that will test information flows, techniques and measures currently in use, decision-making, and future resource investment planning in the wake of the test incident.

R1.22 Appropriate resources need to be allocated for cybersecurity crisis preparedness exercises. Where funding or resources are currently lacking, international funding may be available.

R1.23 Evaluation should be followed up with training that aims to correct identified problems. The cybersecurity crisis management authority should provide guidance on cybersecurity crisis management planning to ensure that it comprises tasks and objectives that are specific, measurable, attainable, relevant, and time-bound (SMART).

CYBER DEFENCE

R1.24 Ensure the development of a cyber defence component in the national security strategy. This component should consider the threats to national security that might emerge from cyberspace.

R1.25 At the state level, consider establishing cyber operation units in different branches of government and armed forces as appropriate.

R1.26 Develop a communication and coordination framework for cyber defence in response to malicious cyber-attacks on military information systems and critical infrastructure.

R1.27 Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.

COMMUNICATIONS REDUNDANCY

R1.28 Establishing redundancy where it does not currently exist for systems supporting the core functionalities of CI organisations should become a priority for international partners. Identification of these systems should be the product of asset mapping during risk assessment.

R1.29 Shortcomings identified during emergency response exercises and drills should be remedied through training and resource allocations where possible.

R1.30 Where approaches have proven effective toward assuring communications redundancy under challenging conditions, these approaches should be shared with international partners, e.g. via publicly available reports (or secure communications channels where the subject matter is sensitive for some reason).

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including users. The days in which cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programmes for users – systems that can be used easily and be incorporated in everyday practices online.

This dimension reviews important elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This dimension also entails the existence mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D 2.1 CYBERSECURITY MIND-SET

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-up - Formative

The cybersecurity mind-set in Bosnia and Herzegovina is still in an early, nascent state of development. Participants from both the public and private sectors described an overall low level of awareness of the values, attitudes and practices necessary for a healthy cybersecurity ecosystem. This lack of awareness is the result of limited knowledge of existing cyber threats,

which in turn stems from a lack of harmonisation in the legislation, in established mechanisms for awareness-raising and most saliently in the challenge of designating a cohesive implementation lead for cyber issues in Bosnia and Herzegovina.[50]

Indeed, as we have explained elsewhere in this report, BiH is characterised for having a complex security management structure split between the state, the entities and the district levels.[51] The implications of this unique organisation are twofold: on the one hand, best practices are mostly seen in IT-related areas of work and in the finance sector. On the other hand, this also means that awareness-raising is also devolved: the State slowly taking measures for improvement, though struggling for centralised cohesion; the private sector being close behind. Banks, for example, have the best coordination and it is through this coordination that higher awareness exists. Other industries, however, are not fairing as well.

On a government level, representatives emphasised the need to prioritise cybersecurity across the public sector and recognised the demand for a shift in the mindset of public officials towards more embedded cyber-aware practices. Officials from leading government agencies remarked that, in general, IT security departments have begun to place priority on cybersecurity, by identifying risks, threats and the need for educational provisions; but that this awareness does not systematically spread to other government departments within different ministries at both the Federal and entity levels. Participants identified the existence of basic security steps, such as the use of passwords to log into computers, the difference between the intranet and the internet, and of a number of policies delineating guidelines for the use of equipment, but the level of follow-through of these practices is not measured or known. Training is provided in relation to these protocols, and some ministries, like the Ministry of Communications and Transport at the state level are working towards the adoption of policies of information security management, which is expected to outline certain measures and guidelines that will improve the cybersecurity mind-set of the country's government. These policies are envisioned for the year 2020.

In contrast, in the private sector, leading firms have begun to place priority on a cybersecurity mind-set by identifying high-risk practices. Participants agreed that private companies (especially major telecommunication providers and international ICT companies, as well as financial institutions), have a good understanding of cybersecurity risks and protective measures, and that they actively seek improvements in their company habits by staying informed about the latest trends in the market. This is particularly true of large service providers, who in addition seek to appoint cybersecurity trained professionals and offer training programmes and materials to improve cybersecurity practices. In these companies, internal security policies are at a high level and participants observed that companies make use of electronic communication. However, the same was not observed in the case of

[50] Baraković, S. and Jasmina Baraković Husić (2015) "'We have problems for solutions': The State of Cybersecurity in Bosnia and Herzegovina". *Information & Security: An International Journal, vol. 32* [online] Available at http://dx.doi.org/10.11610/isij.3205 (Accessed 14/11/2018), p.4.
[51] Baraković, S. and Jasmina Baraković Husić (2015) "'We have problems for solutions': The State of Cybersecurity in Bosnia and Herzegovina". *Information & Security: An International Journal, vol. 32* [online] Available at http://dx.doi.org/10.11610/isij.3205 (Accessed 14/11/2018), p.5-6.

medium-sized companies where the mind-set is perhaps developing, but where the level of protection continues to be rather low. These companies are faced with important cyber threats, such as international phishing scams and ransomware (which participants referred to as the 'Nigerian scam', implying international phishing scams which first originated in Nigeria).[52]

Much like most of the public and private sectors, internet users in BiH do not generally have a developed cybersecurity mindset or systematic good habits surrounding their behaviour online. A limited proportion of Internet users have begun to place priority on cybersecurity, by identifying risks and threats; and these, according to participants, vary significantly and in particular, in relation to age. The younger population is deemed to be better aware of the threats posed by the internet, whereas the elderly evidence a more relaxed attitude and lack of attention to their behaviour online, which was also linked to lack of knowledge. One of the examples shared was that among the older population, passwords are often used but then quickly forgotten, making this sector of the population more vulnerable to attacks.

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Stage: Start-up - Formative

Angriawan and Thakur (2008) define online trust as 'when a consumer has confidence in an e-merchant's reliability and integrity to perform online transactions successfully.'[53] These transactions can involve the exchange of money, but also more widely, the sharing of information that may or may not be sensitive.

The results of this assessment have shown dissenting views when it comes to users' overall trust and confidence in the internet. Some participants indicated that Bosnians are not trusting in the government, an attitude that also limits their ability to trust in the limited e-government services available. Bosnians feel insecure about the services available to them, which was remarked as most likely linked to an overall lack of awareness and understanding of the possible threats – lack of ICT literacy. This becomes particularly salient when the general population is compared to the ICT experts who participated in the assessment who declared having some degree of trust in online services. But more than 90% of the population lack

[52] Scamwatch. Nigerian scams. Available at https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams (Accessed 14/11/2018)
[53] Angriawan, A., Thakur, R. (2008). A Parsimonious Model of the Antecedents and Consequence of Online Trust: An Uncertainty Perspective. Journal of Internet Commerce, Vol. 7, No. 1, 2008, pp. 76. (Accessed 14/11/2018)

internet competency, which coupled with a high unemployment rate (35.33% in September 2018)[54] makes even the use of e-government and e-commerce services limited. Critical infrastructure professionals indicated, for example, that many people do not use online shopping – even though there is some provision available – because they do not know how to use it or do not possess credit cards to make online purchases. The use of e-government and e-commerce services appears to be more popular with those who already work in ICT, those with higher power of acquisition or those with ICT literacy skills (particularly young people under 25).[55] And within those that do use the internet to meet their daily needs, there appears to be an overall use of both local websites and international websites (such as Amazon, Facebook, etc.).

E-commerce services are often offered in an unsecure environment. They are being provided to a limited extent and when provided, a limited proportion of users trust in the secure use of e-commerce services. Therefore, for users to realise the benefits of e-government and e-commerce services, they must also be aware of their existence. The lack of awareness of this offering, coupled with the lack of e-skills (especially for the elderly), is paramount to even consider the importance of developing information security online, as an important component of trust and confidence in the Internet.

By contrast, other participants pointed out that internet users do trust, perhaps 'too much' in the services provided by the government online, as well as those of the financial sector (banks, primarily), therefore suggesting that user trust and confidence on the Internet is mostly at a start-up level. At the same time the country is beginning to show elements of the formative stage, whether this is the result of too much 'undue' trust or of lack of trust. For example, most Internet users appear to have blind trust on websites and regarding what they see or receive online. Operators of Internet infrastructures consider measures for promoting trust in online services; however critical infrastructure providers noted that the expansion of these services and the trust that is required poses a challenge for elderly people.

At the same time, it was noted that a very limited proportion of Internet users critically assess what they see or receive online believing that they have the ability to use the Internet and protect themselves online. A limited proportion of users trust in the secure use of the internet based on indicators of website legitimacy. Operators of Internet infrastructure develop measures to promote trust in online services but have not yet enjoyed high take-up. On a governmental level, there has been recognition of the need to improve trust and confidence of the Internet. This has been addressed by anti-corruption and e-transparency efforts, as well

[54] Trading Economics (2019) Bosnia and Herzegovina Unemployment Rate. Available at https://tradingeconomics.com/bosnia-and-herzegovina/unemployment-rate (Accessed 15/12/2018)
[55] Serife O. & Obralic Merdzana, Cickusic Emir, Ejupi Dzenis, Dzaferovic Emir (2012). E-Commerce in Bosnia and Herzegovina [online]. Available at: eprints.ibu.edu.ba/id/file/18617 (Accessed 15/12/2018)

as by joining the Open Government Partnership[56] through the Ministry of Justice and developing an action plan around it.[57]

When it comes to user trust in e-government services, the government offers limited e-services in a decentralised way (consistent with the country's complex governance structure). One advantage it does have is that it is able to 'serve everyone in their own language and alphabet', even though it has not publicly promoted the necessary secure environment.[58] Bosnia and Herzegovina does not yet have e-signatures available universally, though the service exists.[59] With the exception of the Agency for Identification of Documents, all documentation in the country needs to be verified by hand. A certifying body at the national level does not exist, despite the Law on Electronic Signature of BiH that promotes the certification of signatures being adopted in 2006 . Since there is no institution in BiH that has the authority to issue certificates confirming the authenticity of electronic signatures, the Law on Electronic Signature has not been implemented yet. Also, the adoption of such regulations is complicated through the political dynamics in the country and the slow pace of development of the legislation.

At the same time, government plans to increase e-government provision, but also recognises the need for the application of security measures to establish trust in these services. In 2015, Bosnia and Herzegovina registered as performing less well than the regional average on the provision of e-government services.[60] According to this study, although BiH was then in the process of building of a Strategy For Information Society Development, in line with the Digital Agenda of the Europe 2020 Strategy, the country had not yet designated a state government body to coordinate the establishment of e-government services and instead recognised several players involved in e-government, thus hindering the country's ability to effectuate this plan.[61]

Additionally, the need for security in e-government services is recognised by stakeholders and users. According to Stojanović and Musić (2018), the best examples of e-government service websites in the FBiH are: the Institute of Health Insurance and Re-insurance Fund of Federation of Bosnia and Herzegovina, the Federal Administration for Geodetic and Property Relations, the Tax Administration Federation of Bosnia and Herzegovina, and the best examples of the e-Government services websites in the Republic of Srpska: the Health Insurance fund of Republic of Srpska, the Electronic Land Registry of the Republic of Srpska, the Tax Administration Republic of Srpska, and the public administration of the Republic of

[56] Open Government Partnership. Available at https://www.opengovpartnership.org (Accessed 14/11/2018).
[57] ReSpa (2015). E-government Analysis: From E- to Open Government [online]. Available at: https://www.respaweb.eu/download/doc/eGov++From+EGovernment+to+Open+Government.pdf/d3ab1cd43fa4cd3071be9cea7e4b0cd3.pdf (Accessed 14/11/2018), p.44.
[58] Ibid.
[59] Ibid.
[60] Ibid.

[61] Ibid.

Srpska.[62] The basic limiting factor analysed by the article of Stojanović and Musić was the lack of political agreement on further development of e-government, though improvements were seen to be made in this study since the 2016 report.[63]

The private sector recognises the need for the application of security measures to establish trust in e-commerce services. Some e-commerce services are informing users of the utility of deployed security solutions. But they are very far from having a centralised portal for all users.

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Start-up

In Bosnia and Herzegovina, Internet users and stakeholders within both the public and private sectors recognised that there is no systematic user understanding of personal information protection online. These participants remarked that only a small proportion of the population – and in most cases, these are people who already work in the cyberspace – practice caution when sharing information online or using online services. Most people share information in social networks with little concern, unaware of the degree to which sensitive personal information should be kept private. This included examples of pictures of small children and credit card numbers posted online. Participants pointed to a lack of awareness-raising campaigns within societal advocacy groups and public entities, as the main reason behind poor user understanding of personal information protection online. They also agreed on the importance of the implementation of mechanisms that would ensure people's understanding of good practice around data sharing and data usage, but remarked that a lack of political will slowed down this process, resulting in not only Bosnians being unaware of the risks that their publicly available data face, but also lack of trust in using any online technology.

A few exceptions were mentioned in the case of government ministries where good practices and discussions have begun regarding the protection of personal information, and the balance between security and privacy, but this has not resulted in concrete actions or policies. Despite the fact that the law is Bosnia and Herzegovina prescribes that people should not share or

[62] Stojanovic, Z. and Mehrudina Music (2018). Development of E-government in Bosnia and Herzegovina. The International Journal for interdisciplinary studies 2018. Vol. 8 (1) 70-76) [online]. Available at https://human.ba/wp-content/uploads/2018/04/Article-10.pdf (Accessed 14/11/2018)
[63] Ibid.

have access to personal data that they are not supposed to have, participants recognised that the 'human factor' often transcends good practice and personal information is shared among services and institutions when these should not be shared. In the context of developing a National Cybersecurity Strategy in Bosnia and Herzegovina, discussions involving multiple stakeholders around how personal information should be handled online have begun, but no privacy standards are in place.

GDPR is a topic that is becoming more and more present in Bosnia and Herzegovina in the context of the country's candidature to join the European Union. Members of the public sector expressed knowledge of the importance of abiding by the rules of GDPR for the EU candidature and the country is taking steps in solidifying its prescription to those rules, though it remains slightly obscure still.

2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning as channels for users to report internet related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Formative

The main reporting entity in Bosnia and Herzegovina, both at the entity and cantonal levels, is the police. Each of the two entities, the FBiH and RS has their own police force governed by the Directorate for Coordination of Police Bodies of BiH. In the latter, this is a central force covering the whole entity, in the former a specialist force covering specific crimes and those crimes that cross internal, Cantonal, borders. In the FBiH, there are ten Cantonal police forces, each under a Cantonal Ministry of the Interior. The District of Brčko also has its own police force. At the level of the central state, BiH also has a police agency focused on Counter Terrorism, Organised Crime and crime crossing international borders, the State Investigation and Protection Agency (SIPA), and a State Border Service. Although agreement was reached on unifying the police forces, much like the armies were unified, it has yet to be realized.

The police have been the main reporting mechanism on cybersecurity known to participants from both the public and private sector, though those from the public sector pointed to the existence of other mechanisms, such as the homepage of the Ministry of Interior a the state level, which has a special section on high-tech criminality. According to one participant, this page allows for a direct contact with the department and receives reports on a daily basis. Banks, on the other hand, are known to have their own online reporting mechanisms for small incidents, though for more serious incidents, the police are still the main point of contact.

The reality remains that law enforcement in BiH assumes most of the responsibility when addressing online fraud, cyber-bullying, child abuse online, identity theft, privacy and security

breaches and other incidents. This assessment did determine that the existing channels of reporting, particularly between entities and regions is not coordinated and is used in an ad-hoc manner. The same was observed in relation to the promotion of the existing reporting channels – some participants' lack of systematic awareness about these reporting mechanisms showed that their promotion is scarce and ad-hoc. According to participants themselves, this is due to decentralised channels of communication.

D 2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Start up - Formative

In Bosnia and Herzegovina, cybersecurity issues are overall insufficiently reported across mainstream media both online and offline. This state of affairs spans from the media coverage of cybersecurity incidents to the broader discussion of cybersecurity topics online. The only exception appears to be the case of international news reporting (one participant mentioned Estonia's cyber-attack in 2007). It was noted, however, that when comparing traditional 'offline' news reporting with social media information sharing, cyber incidents were definitely more present in the latter than in the former – partly and potentially due to flexibility and simplicity in sharing information online. Users use social media and social networking more generally to pass on information and get involved in grassroot causes, but not necessarily in relation to cybersecurity.[64] People who are interested in cyber issues are seen to join different discussion groups, particularly on Facebook. Participants considered the lack of interest in sharing cybersecurity related information online and offline, as linked to a general lack of awareness about the existing issues. There was also a consensus that media and social media do not play a significant role in raising awareness about the issues, but that they should.

RECOMMENDATIONS

[64] Global Information Society Watch Report (2011). Bosnia and Herzegovina: is online media and ally for social justice? Trapped between hate and inflammatory Speech [online]. Available at https://www.giswatch.org/en/country-report/freedom-expression/bosnia-and-herzegovina (Accessed 14/11/2018).

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *cyber culture and society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MIND-SET

R2.1 Leading government agencies at the State level need to place priority on cybersecurity, by identifying risks and threats, but also by mandating that the same priority is placed at the entity and district level, in the Federation of Bosnia and Herzegovina, the Republic of Sprka and the Brcko District.

R2.2 Use the leverage of local governments, at cantonal and/or municipal level to educate the public on the nature and consequences of cybercrime in BiH.

R2.3 Consider setting up a multi-stakeholder (businesses, law enforcement agencies, and academia) and multi-governmental groups (from the different administrative structures) to think through cohesive measures (projects and initiatives) and campaigns to raise the public's understanding of cybersecurity risks and threats.

R2.4 Identify vulnerable groups and high-risk behaviour across the public, in particular children and women, to inform targeted, coordinated awareness campaigns that might contribute to users developing critical awareness around possible risks.

R2.5 Encourage private sector institutions (beyond the banking and telecoms sector), and especially those offering e-commerce services to prioritise a cybersecurity mindset by developing training programmes, materials (i.e. brochures, guide books) and sharing information in-house but also across organisations and sectors on incidents and best practices to improve cybersecurity practices.

TRUST AND CONFIDENCE ON THE INTERNET

R2.6 Develop and disseminate surveys in order to understand, at a National level, Internet users' level of Trust and Confidence on the Internet, in E-government and E-commerce services.

R2.7 When introducing e-government services for citizens, implement security measures from the beginning to build trust and uptake by citizens, companies, and other users.

R2.8 When introducing e-government services for citizens promote their use through a coordinated programme, including the compliance to web standards that protect the anonymity of users.

R2.9 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.10 Ensure that security measures are in place for existing e-government services for businesses and public organisations.

R2.11 Encourage government leaders to use social media (e.g. Facebook, Twitter, YouTube, Instagram) and promote the use of e-government services on their social media profiles in a fun and creative way, such as through videos and infographics. Users are more likely to use e-government services if politicians/leaders use social media responsibly.

R2.12 Encourage government leaders to engage with the public via social media channels in order to create trust and show that they act in the public's interest. These platforms can be used in an efficient way to communicate their message and demonstrate their commitment to giving back to the communities.

R2.13 Consider educating the public by developing an effective Cybersecurity Communication Strategy/Plan (e.g. strategic approach to cyber crises, promoting the benefits of using e-government services and suggesting deadlines to register).

R2.14 Promote the implementation of user-consent policies by Internet operators.

R2.15 Encourage internet service providers (ISPs) to establish programmes that promote trust in their services based on measures of effectiveness of these programmes.

R2.16 To promote trust of users in e-services inform users about the utility of deployed security solutions.

R2.17 Encourage the development of e-commerce services with emphasis on the need for a security (e.g. use of SSL encryption, post trust certificates/logos of third-party authentication services on the homepage).

R2.18 Encourage chief executive officers (CEOs) of companies to use social media platforms in order to create trust with their customers and increase transparency. Customers are more likely to use e-commerce services and products if the CEO of their preferred brand uses social media.

R2.19 Ensure that the private sector apply security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

R2.20 Encourage users to access the terms and conditions for using e-commerce services.

R2.21 To promote trust of customers in e-commerce services post customer reviews (both good and bad) and testimonials.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.28 Continue programmes in cooperation with NGOs and support existing efforts by stakeholders to raise user awareness of online risks. Promote measures available to protect privacy and enable users to make informed decisions when and how they share their personal information online.

R2.29 Encourage a public debate on social media platforms and in the traditional media (TV and print) regarding the protection of personal information and about the balance between security and privacy to inform policymaking.

R2.30 Develop a Code of Practice on Protecting Personal Information Online in consultation with multiple stakeholders that can be distributed within the public (e.g. in primary and secondary schools).

R2.31 Establish e-signature across the country in order to enable further e- service development. Consider starting to deploy the e-signature developed for the Council of Ministries to other agencies and ministries and allow government to communicate electronically internally. A further stage would be to deploy e-signature to citizens and businesses as a centralized option using national e-ID or as a mutually recognized e-signature provider between all entities and cantons.

REPORTING MECHANISMS

R2.32 The Open Government Partnership should be embraced with more partners from both private and public sectors. An expanding partnership will help ensure that all public administration in BIH should establish one central place for reporting incidents and for feedback on administration services. Online and regular (mail and phone) channels of communication should be opened to citizens to provide feedback on government work and services.

R2.33 Establish coordinated mechanisms within the public and the private sector allowing citizens to report cybercrime cases, including online fraud, cyber-

bullying, child abuse online, identify theft, privacy and security breaches, and other incidents, in particular affecting women and other vulnerable groups.

R2.34 Provide manuals to educate the public, teachers and parents about the types of cybercrime that can be reported, how to exercise their rights when falling victim to such crimes and how to report it. These can be distributed through local channels at the entity and cantonal levels.

R2.35 Raise awareness about new and existing reporting channels among the wider public and across stakeholder groups and cooperate with the private sector in this regard.

R2.36 At the state level, set up a website at the Ministry of Interior where victims of cybercrime would be able to report to the police by choosing different options: 1) dialling a number in case it is an emergency or the crime is in progress 2) completing an online form for non-emergency crimes or reporting via email. It is important that all reporting channels should offer the victim the option to report anonymously (e.g. anonymous online forms).

R2.37 At the state level, consider establishing the Cybercrime Unit of the Ministry of Interior as the national fraud and cybercrime reporting centre, providing a central point of contact for citizens and businesses.

R2.38 Consider establishing secure two-way information sharing between the Cybercrime Unit and the heads of different entities and cantons.

MEDIA AND SOCIAL MEDIA

R2.39 In cooperation with civil society and media organisations develop programmes and campaigns to raise awareness among media providers and leading social media actors, for instance during the dedicated Safer Internet Day or the Cybersecurity Awareness Month (October) or dedicated web or social media sites on this topic.

R2.40 Enhance the understanding of cybersecurity among media providers (e.g. journalists and editors) and facilitate a more active role of media in conveying information about cybersecurity to the public.

R2.41 Encourage media content providers to disseminate information on good (proactive) cybersecurity practices that users can pursue to protect themselves or to respond to cyber incidents. This could stimulate social media discussions on the topic.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D 3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Start up

Awareness of cybersecurity risks and threats in Bosnia and Herzegovina is still low at all levels of society, and our research identified that awareness of cybersecurity threats and vulnerabilities across all sectors is currently in the initial stages of discussion. Participants admitted that awareness raising is not a priority for government institutions, in part because there is a lack of knowledge around what possible risks and threats might exist. Awareness-raising programmes, courses, seminars and online resources are available for target demographics from public, private, academic and/or civil society resources, but no coordination or scaling efforts have been conducted. For example, participants indicated differences between the central State level and the entity level, revealing that in Republic of Srpska some programmes are in existence for the general public, but that a unified coalition around awareness raising is still lacking on the national level. Some school programmes are delivered on the initiative of specific teachers; and October is not considered Cyber-Awareness month like it is in a number of other European countries. There is only one event

in October 2018 in relation to cyber-awareness month, and it is a Training on Raising Security Awareness by the Ministry of Internal Affairs of the Zenica-Doboj Canton.[65]

Additionally, when present, awareness-raising programmes appear to still be informed by international initiatives, like the one revealed by one participant, which involves a proposal for a digital skills training campaign of a value of £10M coordinated in the Western Balkans by the British Council. It is worth noting that this initiative is yet to be implemented (the details of this campaign are not known and whether awareness-raising is one of the topics covered, is yet to be known. The goal of the initiative is to help build digital skills for young people in the Western Balkans and employment rates for its young people).[66]

None of these programmes or campaigns appear to be currently linked to the country's efforts towards a National Strategy. That being said, in June 2018, the ITU-D in cooperation with the Communications Regulatory Agency (CRA), the Ministry of Security of BiH and the Ministry of Transport and Communications of BiH disseminated a statement that proposes to develop and implement regional and national awareness-raising campaigns throughout 2018 and 2019 in order to raise awareness in the community about cybersecurity threats, with a focus on young people.[67] The purpose of this initiative is specifically intended to contribute to enhance trust and confidence in the use of information and communication technologies in Bosnia and Herzegovina.

Awareness raising on cybersecurity issues for executives is limited, though more systematically present than in the wider population, particularly in the case of multinational companies or executives from the finance sector, which do have more specific guidelines to follow. For example, participants described that in the banking sector, workshops are delivered on a regular basis. They address cyber risks in relation to social engineering and the techniques used by cyber-criminals to manipulate people online. Sessions and workshops are also delivered to make executives aware of cyber policies and procedures. External companies such as NESECO founded in 2010, offer security awareness training to members of the public.[68]

On the other hand, in the majority of companies, executives are not yet always aware of their responsibilities to shareholders, clients, customers, and employees in relation to cybersecurity. At times, they are made aware of general cybersecurity issues, but not how these issues and threats might affect their organisations. Select executive members are made aware of how cybersecurity risks affect the strategic decision making of the organisation, particularly those in the financial and telecommunications sectors. Awareness-raising efforts

[65] ENISA. Training on Raising Security Awareness. Activities from Bosnia and Herzegovina. Available at https://cybersecuritymonth.eu/ecsm-countries/bosnia-and-herzegovina/training-on-raising-security-awareness (Accessed 15/12/2018)

[66] UK Government (2018) Foreign Secretary to announce £10 million commitment to build digital skills in the Western Balkans. Available at https://www.gov.uk/government/news/foreign-secretary-to-announce-10-million-commitment-to-build-digital-skills-in-the-western-balkans?utm_source=defcd7c5-544e-4316-ae41-3235a384110d&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate (Accessed 15/12/2018)

[67] ITU Regional Development Forum for Europe (2018). "Contribution by communications Regulatory Agency of Bosnia and Herzegovina: Statement of the situation and proposal of activities to enhance trust and confidence in the use of information and communication technologies" [online]. Available at https://www.itu.int/en/ITU.../Bosnia%20and%20Herzegovina%20EUR4received.pdf (Accessed 15/12/2018)

[68] Neseco. Available at https://www.neseco.ba/trainings (Accessed 15/12/2018)

of cybersecurity crisis management at the executive level are still reactive in focus, responding to specific incidents, rather than being preventative. Participants expressed that executive have a noted interest to invest in solving issues when they occur rather than implementing measures to sensitise their employees before incidents happen.

D 3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Start-up - Formative

According to the National Cyber Security Index (October 2018), drawn up by the e-Governance Academy in Estonia, which places Bosnia and Herzegovina in the 45th overall position at the National level, and 13th globally, the country does not register any cyber safety competencies in primary, secondary or bachelor's education, but registers at least one accredited programme at master's[69] and doctoral[70] levels.[71] This section of the report will elucidate the provisions available in these different categories and also provide an assessment around the existing uptake of the services provided.

At primary and secondary levels of education, participants explained that cybersecurity-related topics include less than a year of lessons, concentrated on no more than one module within existing Information Technology courses. Some schools also provide programmes to teach educators and schoolchildren about safety on the internet; in some cases, this work is being done though NGOs. The education in Bosnia and Herzegovina is not offered at a state level, it is considered very fragmented in relation to various levels of government in BiH, which inevitably affects consolidated provisions. This is also likely due to the fact that cybersecurity educators available are few and far between there are no systematic qualification programmes for educators. However, qualification programmes for cybersecurity educators are being explored to support the small cadre of existing professional educators.

At the higher education level, Bosnia and Herzegovina has eight public universities: University of Sarajevo, University of Banja Luka, University of East Sarajevo, University of Mostar, University of Tuzla, University of Zenica, University of Bihać, and University Džemal Bijedić of Mostar. Of the three that were represented at the review, there appeared to be consensus in that universities in BiH offer some undergraduate and postgraduate cybersecurity courses as

[69] American University in Bosnia and Herzegovina. Master's Degree Program in Cyber Security. Available at https://aubih.edu/en/fst-masters-cs-program.html (Accessed 13/12/2018)
[70] American University in Bosnia and Herzegovina. Doctoral Degree Program in Cyber Security. Available at https://aubih.edu/en/fst-doctoral-cs-program.html (Accessed 13/12/2018)
[71] NCSI (2018) Bosnia and Herzegovina [online]. Available at https://ncsi.ega.ee/country/ba/ (Accessed 13/12/2018)

part of their Faculty of Engineering (engineering is still the term used to refer to computer systems, electrical engineering or computer science). Courses also exist at a doctoral level, but are much scarcer. These courses cover topics such as information security, security and safety in cyberspace, security culture awareness, computer crime and cyber law. This shows that computer science courses that may have a security component are offered, but no cybersecurity-related courses are taught. Some educational courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet available.

The University of Sarajevo, for example, recently launched Bosnia and Herzegovina's first Internet exchange platform, in order to create opportunities for the 'the joint organization of research activities, symposia, conferences, seminars as well as through studying problems of common interest and finding the best ways of solving them.'[72] The University also offers some courses that include summer school and short-term courses. As undergraduates, students can choose cybersecurity training and education related to law enforcement and criminology. In order to be accredited they must complete the third year of University. At a postgraduate level, a high level of technical knowledge is required, making the uptake of the courses more limited. Students at a Masters' level are able to choose between two courses at the Department of Telecommunications (in the first year), which cover mostly cryptography, and in the second year, they are able to select a course in the Department of Computing. But these are all elective modules and not compulsory for one to be able to graduate with a degree in Computer Science. Participants from the education sectors shared that these courses usually attract between two to twenty students a year.

It was not clear from the review whether students at any of the levels of education described above, showed demand for cybersecurity education. In terms of administration, the need for enhancing cybersecurity education in schools and universities has been identified by leading government, industry, and academic stakeholders. Schools, government, and industry collaborate in an ad-hoc manner to supply the resources necessary for providing cybersecurity education. A national budget focused on cybersecurity education is not yet established.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

[72] University of Sarajevo (2018) Cooperation between the Ministry of Communications and Transport of BiH and the University of Sarajevo. Available at http://www.unsa.ba/en/novosti/cooperation-between-ministry-communications-and-transport-bih-and-university-sarajevo (Accessed 13/12/2018)

Stage: Start-up – Formative

Bosnia and Herzegovina offers some cybersecurity training programmes to professionals working in different sectors, but this provision appears to be ad-hoc, and not readily recognised by the government.[73] This lack of recognition was pointed out as one of the factors behind the low number of cybersecurity-aware experts and the prevalence of software developers. Participants expressed the need for this training to become more systematically coordinated and recognised on the national level. According to Baraković and Baraković Husić (2015), however, this coordination is currently hampered by the lack of a 'central contact point on the state level' and 'extremely weak cooperation between institutions and universities' to successfully apply for and adequately distribute investments for cybersecurity training and cooperation.[74] Participants also indicated that they hoped this might change with the development and implementation of the country's National Strategy. Currently, only three people in the country have gone through accredited cybersecurity training; and among those three, only one is a Certified Information Systems Security Professional (CISSP). It was indicated that in the market for professional education and training there is a space and need for cyber awareness, with cybersecurity focused on data protection being an area identified as particularly lacking, especially on a regional level. There are some projects in critical infrastructure but there is a gap on the ground inside the political system to strengthen that space.

Within public institutions, training on cybersecurity issues both for IT and general staff is limited and often takes place contingent on the incentive of the respective management in the institution. At the State level, initiatives exist, but these rely on individual institutions expressing the need for adequate training, and for it to be then carried out. The trainings offered can vary between general cybersecurity training and certified courses, but resources still appear to lack. In order to receive appropriate certification, accredited courses require that the member of staff passes an exam.

In the private sector, though training appears to be available in some institutions, some participants remarked that certification is often not mandatory. Some certification is available from companies such as Microsoft and Cisco, though these tend to be more expensive. Other local companies such as NESECO also provide accredited services.[75] The main training available is in information security; certification as an information security auditor does not yet exist in Bosnia and Herzegovina. The ability to address an incident is prioritised over the employee's accreditation in any particular area. Empirical knowledge is seen as sufficient and formal training is not a requirement. Companies sometimes also opt for outsourcing the work in response to a specific incident, rather than to preventatively invest in staff that will be able to keep the knowledge in-house and later also be able to transfer it to other members of the team.

[73] ITU (2018). Readiness Assessment Report to Establish a CIRT Network in Bosnia and Herzegovina, p.24-25.
[74] Baraković, S. and Jasmina Baraković Husić (2015). "'We have problems for solutions': The State of Cybersecurity in Bosnia and Herzegovina". *Information & Security: An International Journal, vol. 32* [online] Available at http://dx.doi.org/10.11610/isij.3205 (Accessed 15/12/2018), p. 16.
[75] Neseco. Available at https://www.neseco.ba/trainings (Accessed 15/12/2018)

In contrast, exceptions appear to exist in the telecoms sector where there is significant money invested in the training of its people whether it is in person, online or abroad. These companies do seem to invest in their employees in the hopes that this knowledge will stay in-house and later transferred to others.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to Bosnia and Herzegovina. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

AWARENESS RAISING

R3.1 Appoint a dedicated body within each of the entities of BiH and BD with a mandate to develop and implement a planned national cybersecurity awareness-raising programme alongside a single designated body at the state level, as well. The designated body at the state level should coordinate and cooperate with key stakeholders, in particular those who participated in the review, representing private sector, civil society, and international partners and government bodies who will be responsible for delivering the programmes to the rest of the population. This could be done through efforts coordinated with other Western Balkan countries, so common threats are addressed.

R3.2 At the entity and canton levels and BD, implement portals to disseminate materials for various target groups. Ensure aligning of this effort with existing platforms to avoid duplication. This could be coordinated at the state level, but managed locally and targeted to the specific audiences of the individual entities and cantons.

R3.3 Coordinate an awareness-raising effort, for instance through the dedicated cybersecurity awareness month (in October) and develop materials for specified target groups and sectors, based on international good practice. This could be coordinated locally, but overseen by a national body.

R3.4 Once the single dedicated body at the state level is established, it should be responsible for integrating cybersecurity awareness-raising efforts into ICT literacy courses and build upon existing initiatives as established vehicles for cybersecurity awareness-raising campaigns. Particularly, the initiatives already identified by the Communications Regulatory Agency (CRA), the Ministry of Security of BiH and the Ministry of Transport and Communications of BiH to

continue their work throughout 2019 using the recommendations offered by this report.

R3.5 The regional and national awareness-raising campaigns proposed by ITU-D should be extended and directed to the general public, with a focus on women and other underrepresented groups. This programme should be in coordination with other ongoing initiatives in order to make the awareness-raising more effective.

R3.6 Establish metrics for assessing cybersecurity awareness raising programmes and ensure that evidence of application and lessons learnt feed into existing and newly-developed programmes.

R3.7 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors, as this group is usually the final arbiters on investments into security.

FRAMEWORK FOR EDUCATION

R3.8 Coordinate efforts between universities to offer joint lecture series or seminars to increase the knowledge exchange in cybersecurity within the country. This could also open discussions for best practices in cyber education and awareness-raising.

R3.9 Develop partnerships for the development of interfaces for research, innovation and interaction between universities and the private sector.

R3.10 Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators to ensure that skilled staff are available to teach newly-formed and existing cybersecurity courses. Consider invited guest speakers from other countries in the region or further afield.

R3.11 Include cybersecurity modules and courses as part of the core curriculum of undergraduate level education in all Science and Engineering departments at universities. Cybersecurity orientation courses should be integrated in all university courses.

R3.12 Create cybersecurity education programmes for non-cybersecurity or computer science experts and make them available as electives at universities and other higher education bodies, for those interested more generally in this topic. This might also create opportunities in the future for interdisciplinary work, thus enhancing the overall education framework in BiH.

R3.13 Collect and evaluate feedback from existing students on the type of cybersecurity courses they are interested in further development and enhancement of cybersecurity course offerings.

R3.14 Consider promoting cybersecurity as a career in schools and universities at both state and entity levels and BD.

R3.15 Allocate national budget for cybersecurity education at both state and entity levels and BD.

R3.16 Develop the opportunity for scholarships in cybersecurity studies across all levels of higher education. These could be sought through partnerships with international partners and donors.

R3.17 Create initiatives to advance cybersecurity education in the primary and secondary school curricula, through compulsory courses on cybersecurity but also through events such as the Awareness Month, with a specific focus on topics relevant to young people.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.18 Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals. Cooperate with the private sector to develop those offerings. These offerings could be organized across jurisdictions, cantons, entities and BD in order to share experiences.

R3.19 Provide trainings for experts on various aspects of cybersecurity, such as technical trainings in data systems, tools, models, and operation of these tools. Make this part of the standard training for any IT professional in both public and private sectors. These trainings could include:

a) Dealing with electronic devices and recognition of devices which may contain evidence of crime.
b) Search of computers and other electronic equipment (mobile phones, etc.).
c) Analysis of digital evidence and its presentation.
d) Use of the internet as an open source tool in investigation.
e) Interception of electronic messages.
f) Training on various types of cybercrime including paedophilia.
g) IT system protection and security.

R3.20 Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

R3.21 Establish continuous training for IT employees and general employees regarding cybersecurity issues. The framework of this training could be developed to meet particular needs of the organization, depending on the level of vulnerability to which they are exposed. Train-the-trainer opportunities should also be considered within the same organisations.

R3.22 Within the police, training on cybersecurity topics should be increased and structurally distributed to the lowest level of police personnel.

R3.23 Promote international cybersecurity certification courses and subsidize the high cost of such courses.

R3.24 Create incentives for cybersecurity experts to stay in the country and get more involved in cybersecurity matters, including creating a business environment, which fosters innovation and entrepreneurship.

R3.25 Promote the recognition of professional cybersecurity training programmes to government decision makers.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Start-up – Established

Bosnia and Herzegovina (BiH) has a complex system of governance that is reflected in the existing legislation of the country. BiH is composed of the Federation of Bosnia and Herzegovina (FBiH), the Republic of Srpska (RS) and the Brčko District (BD), which are self-governing entities each with its own Criminal Code and Criminal Procedural Code that address offences related to cybercrime.[76]

At the state level, the Criminal Code and Criminal Procedural Code focus on tackling the most serious criminal offences such as organised crime and crimes against humanity. Issues related to cybersecurity and cybercrime are therefore dispersed under four Criminal Codes and Laws on Criminal Procedure (one at the state level, two at the entities' level and one at BD).

[76] Murtezic, A. (2014) Assessment of compliance of the criminal codes in Bosnia and Herzegovina with the council of Europe cybercrime convention. Available at http://krimteme.fkn.unsa.ba/index.php/kt/article/viewFile/169/pdf (Accessed 9/11/2018)

Despite the fact that BiH signed the Budapest Convention on Cybercrime in 2005 and ratified it in 2006 (with it entering into force in the same year), the existing legislations at the state level are only partially harmonised and have not fully implemented the provisions of the Convention.[77] Also, adopted or amended legislation does not cover all aspects of cybersecurity, such as human rights protection online and consumer protection and intellectual property online.

The most relevant legislative frameworks related to Bosnia and Herzegovina's internet landscape at the state level are:

Law	Implementation	Article
Criminal Code[78]	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 Code[79]	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[80]	Data security (Partially implemented)	11
Law on the Protection of Classified Data[81]	Protection of classified data (Partially implemented)	77
Law on Communications[82]	Data security	5, 15

[77] DiploFoundation (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. Available at https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf (Accessed 9/11/2018)

[78] Criminal Code of Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina, 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15.

[79] Criminal Procedural Code, Official Gazette of Bosnia and Herzegovina, 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13.

[80] Law on Protection of Personal Information, Official Gazette of Bosnia and Herzegovina, 32/01, 49/06.

[81] Law on Protection of Classified Information, Official Gazette of Bosnia and Herzegovina, 54/05.

[82] Law on Communications, Official Gazette of Bosnia and Herzegovina, 31/03, 75/06.

	(Partially implemented)	
Law on Electronic Signature[83]	Fully implemented	
Law on Electronic Legal and Business Transactions[84]	Fully implemented	
Law on Prevention of Money Laundering and Financing of Terrorism [85]	Partially implemented	26

(Borrowed from Baraković & Baraković Husić[86] (2015) and Council of Europe, Octopus Cybercrime Community, Country Wiki[87])

The failure to fully implement these legislations (see above) suggests the need for the harmonisation of legal regulations in the field of cybersecurity at the state level. Especially, since one of the main foreign policy objectives of BiH is to join the European Union, safeguards will need to be put in place for the enforcement and synchronisation of these legislations.

The Constitution[88] guarantees basic human rights and freedom of speech under Article 2:

Article 2 - Human Rights and Fundamental Freedoms

1. Human Rights

Bosnia and Herzegovina and both Entities shall ensure the highest level of internationally recognized human rights and fundamental freedoms. To that end, there shall be a Human Rights Commission for Bosnia and Herzegovina as provided for in Annex 6 to the General Framework Agreement.

2. International Standards

The rights and freedoms set forth in the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols shall apply directly in Bosnia and Herzegovina. These shall have priority over all other law.

3. Enumeration of Rights

g) Freedom of thought, conscience, and religion.
h) Freedom of expression.

[83] Law on Electronic Signature, Official Gazette of Bosnia and Herzegovina, 91/06.
[84] Law on Electronic Legal and Business Transactions, Official Gazette of Bosnia and Herzegovina, 126/07.
[85] Law on Prevention of Money Laundering and Financing of Terrorism, Official Gazette of Bosnia and Herzegovina, 47/14.
[86] Barakovic, S., & Husic, J. B. (2015) ''We Have Problems For Solutions'': The State Of Cybersecurity In Bosnia and Herzegovina. Information & Security, 32(2), 1. (Accessed 9/11/2018)
[87] Council of Europe. Octopus Cybercrime Community (2017) Bosnia and Herzegovina. Available at https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/bosnia-and-herzegovina?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view (Accessed 9/11/2018)
[88] Constitution of Bosnia and Herzegovina. Available at https://www.wipo.int/edocs/lexdocs/laws/en/ba/ba020en.pdf (Accessed 9/11/2018)

i) Freedom of peaceful assembly and freedom of association with others.[89]

With regards to the freedom of expression (including the press) the Human Rights Report provided by the U.S. Department of State for 2017 stated that the 'governmental respect for this right remained poor', referring to the continued 'intimidation, harassment, and threats against journalists and media outlets.'[90] Despite the fact that freedom of expression is protected by the Constitution, still scarce implementation of the law often leads to undermining the press freedoms.[91] BiH also joined the programme funded by the Council of Europe and the EU on 'Reinforcing Judicial Expertise on Freedom of Expression and the Media in South-East Europe (JUFREX)' that provides training activities for the regulators, journalists and public service media.[92] BiH has not adopted specific legislation on human rights online. According to the Human Rights Report provided by the U.S. Department of State for 2017 there was no violation of Internet freedom by the government.[93]

At the state level, BiH lacks a comprehensive legislation on the protection of children online. Nonetheless, the Ministry of Security of BiH in cooperation with other Ministries and the NGO sector prepared the document 'Action Plan for Child Protection and Prevention of Violence against Children through Information-Communications Technologies in Bosnia and Herzegovina 2014-2015' that has been adopted by the Council of Ministers of BiH.[94] One participant added that many other activities are currently being carried out concerning child protection on the Internet, conducted by the Ministry of Security of BiH and other Institutions. However, at the entity level and BD, legislations addressing the protection of children online were adopted under Articles 211 and 212 of the Criminal Code of the Federation of Bosnia and Herzegovina, Articles 199 and 200 of the Criminal Code of the Republic of Srpska (RS), and Articles 186, 208, 209 of the Criminal Code of the Brčko District (BD).

Articles 211 and 212 of the Criminal Code of Federation of Bosnia (FBiH)

Article 211

Abuse of a Child or Juvenile for Pornography

(1) Whoever photographs or films a child or juvenile with an aim of developing photographs, audio-visual tapes or other pornographic materials, or possesses or imports or sells or deals in or projects such material, or induces such persons to play in pornographic shows, shall be punished by imprisonment for a term between one and five years.

[89] Constitution of Bosnia and Herzegovina. Available at https://www.wipo.int/edocs/lexdocs/laws/en/ba/ba020en.pdf (Accessed 9/11/2018)
[90] US Department of State. Bosnia and Herzegovina 2017 Human Rights Report. Available at https://www.state.gov/documents/organization/277391.pdf (Accessed 14/11/2018)
[91] Ibid.
[92] Council of Europe. Freedom of Expression. Reinforcing Judicial Expertise on Freedom of Expression and the Media in South-East Europe (JUFREX). Available at https://www.coe.int/en/web/freedom-expression/promoting-freedom-of-expression-in-south-east-europe (Accessed 14/11/2018)
[93] US Department of State. Bosnia and Herzegovina 2017 Human Rights Report. Available at https://www.state.gov/documents/organization/277391.pdf (Accessed 14/11/2018)
[94] 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. Available at http://msb.gov.ba/PDF/140605_Nasilje_engleski_SG_ver2.pdf (Accessed 20/03/2019)

(2) Items meant or used for the perpetration of criminal offence referred to in paragraph 1 of this Article shall be forfeited and the items produced by the perpetration of criminal offence referred to in paragraph 1 shall be forfeited and destroyed.

Article 212

Introducing Pornography to a Child
(1) Whoever sells, shows or renders available through a public display or in any other way writings, pictures, audio-visual and other objects containing pornography to a child, or whoever shows him a pornographic show, shall be punished by a fine or imprisonment for a term not exceeding one year.
(2) The items referred to paragraph 1 of this Article shall be forfeited.[95]

Nevertheless, the legislation in FBiH does not connect this offence with the use of computer or internet. In contrast, the Criminal Code of RS specifies more 'severe sanctions for those who commit this crime via the internet.'[96]

At the state level, the legislations addressing intellectual property are covered under Article 243 (Impermissible Use of Copyrights) of the Criminal Code of BiH and the Law on Copyright and Related Rights (2010).[97] The Criminal Code of BiH covers 'a general problem of copyright infringement however excludes reference to IT technologies'.[98] Similarly, at the state level BiH has adopted the Consumer Protection Act (2001), however it lacks provisions that would protect consumers against online fraud and other forms of cybercrime.[99]

During the review, participants referred to the Constitution of Bosnia and Herzegovina as the legislative framework which regulates personal data protection.[100] Based on desk research 'BiH has ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108), and its additional protocol.'[101] Pursuant to the Constitution of BiH and the Convention, the country adopted a Law on

[95] Criminal Code of Federation of Bosnia.Available at http://www.tuzilastvobih.gov.ba/files/docs/zakoni/FBH_CRIMINAL_CODE_36_03.pdf (Accessed 9/11/2018)
[96] Murtezic, A. (2014) Assessment of compliance of the criminal codes in Bosnia and Herzegovina with the council of Europe cybercrime convention. Available at http://krimteme.fkn.unsa.ba/index.php/kt/article/viewFile/169/pdf (Accessed 9/11/2018)
[97] Law on Copyright and Related Rights (2010). Available at http://www.ipr.gov.ba/upload/documents/dokumenti_podstranice/pravna-regulativa/Engleski/IP_Laws_and_Regulations_in_BIH/law_on_copyright_and_related_rights.pdf (Accessed 9/11/2018)
[98] Murtezic, A. (2014) Assessment of compliance of the criminal codes in Bosnia and Herzegovina with the council of Europe cybercrime convention. Available at http://krimteme.fkn.unsa.ba/index.php/kt/article/viewFile/169/pdf (Accessed 9/11/2018)
[99]Consumer Protection Act (2001) Available at http://www.libertasinstitut.com/de/News&Termine/08.BiH.Consumers%20Law%20EN.pdf
[100] Constitution of Bosnia and Herzegovina. Available at https://www.wipo.int/edocs/lexdocs/laws/en/ba/ba020en.pdf (Accessed 9/11/2018)
[101] European Commission (2018) Bosnia and Herzegovina 2018 Report. Available at https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-bosnia-and-herzegovina-report.pdf (Accessed 16/12/2018)

Personal Data Protection in 2006 in order to harmonise it with the EU law required by the Stabilization and Association Agreement.[102,103] This followed the creation of the Personal Data Protection Agency in 2008. According to sources, in 2017 'the Agency received 96 complaints against data controllers in the public and private sector, and carried out 83 inspections.'[104]

The domestic legislation reflects provisions of the Data Protection Directive 95/46.[105] Since the General Data Protection Regulation (GDPR) came into force in May 2018, BiH might want to consider revising the domestic legislation based on the GDPR. This has been confirmed by the participants indicating that the Council of Ministers is in the process of updating the regulation to meet the requirements under the GDPR 2016/679 and the Directive 2016/680.

The following table explains the implementation of substantive law provisions at the entity level and BD in accordance with the Budapest Convention.

Cybercrime Convention directives	**CC FBIH**	**CC RS**	**CC BD**
Article 2 – Illegal access	Article 397	Article 292d	Article 391
Article 3 – Illegal interception	Article 393 p. (2)	Article 174	Article 387 p. (2)
Article 4 – Data interference	Article 393 p. (1)	Article 292v	Article 387 p. (1)
Article 5 – System interference	Article 396	Article 292b, 292đ	Article 390
Article 6 – Misuse of devices	Article 393 p. (5), (6)	Article 281 i 398	Article 387 p. (4), (5)
Article 7 – Computer-related forgery	Article 394 p. (1)	Article 292b, 292g	Article 388 p. (1)

[102] Law on Personal Data Protection (Official Gazette of BiH, No. 49/06) Available at http://www.sipa.gov.ba/assets/files/laws/en/lp49-06.pdf (Accessed 9/11/2018)
[103] Official Journal of the European Union. Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and Bosnia and Herzegovina, of the other part. L 164/2. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22015A0630%2801%29 (Accessed 9/11/2018)
[104] European Commission (2018) Bosnia and Herzegovina 2018 Report. Available at https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-bosnia-and-herzegovina-report.pdf (Accessed 16/12/2018)
[105] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 (Accessed 9/11/2018)

Article 8 – Computer-related fraud	Article 395	Article 292b, 292g	Article 389
Article 9 – Offences related to child pornography	Article 211	Article 199 i 200	Article186 p. (3), 208, 209
Article 10 – Offences related to infringements of copyright and related rights	-	-	Article 256, 257
Article 11 – Attempt of aiding or abetting	Article 28, 31	Article 21, 23, 24, 25	-
Article 12 – Corporate liability	Section 14	Section 14	-
Article 13 – Sanctions and measures	-	-	-

CC (Criminal Code), FBIH (Federation of Bosnia and Herzegovina), RS (The Republic of Srpska) BD (Brčko Distrikt)

(Borrowed from Council of Europe, Octopus Cybercrime Community, Country Wiki)

The following table presents the implementation of procedural law provisions in accordance with the Budapest Convention.

Cybercrime Convention Directives	**CPC BIH**	**CPC FBIH**	**CPC RS**	**CPC BD**
Article16 – Expedited preservation of stored computer data	-	Article 86a	Article 115, 129, 131, 137	-
Article17 – Expedited preservation and partial disclosure of traffic data	-	Article 86a	Article 115, 129, 131, 137	-
Article18 – Production order	Article72a	Article 86a	Article 137	-
Article19 – Search and seizure of stored computer data	-	Article 65	Article 115	-

Article20 – Real-time collection of traffic data	Article 65 p. (6)	Article 130	-Section 17	-
Article21 – Interception of content data	Article 116	Article 130	Section 17	-

CPC (Criminal Procedural Code), FBIH (Federation of Bosnia and Herzegovina), RS (The Republic of Srpska) BD (Brčko Distrikt)

(Borrowed from Council of Europe, Octopus Cybercrime Community, Country Wiki)

For instance, with regards to seizure (Article 19) and interception of content data (Article 21) of the Convention, the Criminal Procedure Codes at the entity level 'comply with the requirement of the Convention since all provisions on actions to obtain evidence, seizure of objects and special investigative measures explicitly include computers and computer systems.'[106]

D 4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Start-up - Formative

Across the criminal justice system, capacities are between start-up and formative stages of maturity in Bosnia and Herzegovina (BiH).

BiH has a very complex organizational criminal justice system, which is determined by a complex constitutional structure of the state. Participants' commentary indicated that institutional capacities to tackle cybercrime issues remain at the entity level and in BD.

At the state level, there is no specialised cybercrime unit to combat cybercrime. The Directorate for Coordination of Police Bodies of BiH within the Ministry of Security only fulfils a coordinating role and manages inter-entity requests.[107]

[106] Murtezic, A. (2014) Assessment of compliance of the criminal codes in Bosnia and Herzegovina with the council of Europe cybercrime convention. Available at http://krimteme.fkn.unsa.ba/index.php/kt/article/viewFile/169/pdf (Accessed 9/11/2018)

[107] Council of Europe (2017) iPROCEEDS. General guide on Protocols on interagency and international cooperation for investigations involving proceeds from crime online. Available at https://www.coe.int/en/web/cybercrime/iproceeds (Accessed 9/11/2018)

Figure 2: Police institutions responsible for tackling cybercrime in BiH

At the entity level, the Federal Police Administration of the Federation of BiH (FBiH) and the Ministry of Internal Affairs of the Republic of Srpska (RS) are in charge of carrying out investigations related to cybercrime and digital forensics.[108] However, within the entities, only the Republic of Srpska has a specialised police cybercrime unit – the Unit for Preventing High-tech Crime located within the Ministry of Internal Affairs – that has sufficient capacity to combat cybercrime and perform digital forensics. Within the Brcko District (BD), specialised investigators within the Police of Brcko District investigate cybercrime cases. [109]

Digital forensics capacity is decentralised among the different institutions at the state, entity level and BD:

<u>At the entity level and in BD:</u>

- Unit for Preventing High-tech Crime[110] formed in 2010 and is located within the Criminal Investigation Department of the Ministry of Internal Affairs of Republic of Srpska
- Police of Brcko District

<u>At the state level</u>

- State Investigation and Protection Agency of BiH
- Border Police of BiH
- Agency for Forensic Testing and Expertise of BiH[111]

[108] Council of Europe. Octopus Cybercrime Community (2017) Bosnia and Herzegovina. Available at https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/bosnia-and-herzegovina?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view (Accessed 9/11/2018)
[109] Ibid.
[110] Ministry of Interior of the Republic of Srpska. Unit for Preventing High-tech Crime. Available at http://mup.vladars.net/vtk/home_en.html (Accessed 9/11/2018)
[111] Council of Europe. Octopus Cybercrime Community (2017) Bosnia and Herzegovina. Available at https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/bosnia-and-herzegovina?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view (Accessed 9/11/2018)

The Unit for Preventing High-tech Crime works closely with the Department for Information Security within the Agency for Information Society of Republic of Srpska (RS) that functions as the first official CERT at the entity level since 2015. Participants noted that computer incidents can be reported to the police and then forwarded to the Ministry of Interior. Since the Criminological Police Sector of the Federal Police Administration of the Federation of BiH does not have a dedicated cybercrime unit and lacks sufficient capacity to investigate offenses committed against computer systems, it relies on the capacity of the Center for Forensics and IT Support[112] within the Federal Police Administration.[113] Similarly, Brcko District does not have a specialised cybercrime unit to carry out cybercrime investigations.

At the state level, it was not possible to obtain a clear picture regarding the capacity of law enforcement, prosecutors and judges, however, participant comments suggested that the judiciary, prosecutors and the police do not have adequate knowledge and skills to investigate cybercrime cases. At the state level, the Agency for Education and Professional Training (AEPTM) established in 2009 is in charge of 'providing research and education in the field of police education and security'.[114] Cybercrime investigations are covered in the training catalogue of the specialist training programmes and available to law enforcement agencies of the Ministry of Security in BiH.[115] The website of the Agency highlights active cooperation with the EU through CEPOL, FRONTEX and TAIEX.[116] Based on sources, the MoU signed between the Ministry of Security of BiH and CEPOL provides a platform to train police officers according to EU standards.[117] However, it was also not clear how the trainings in cybersecurity are disseminated to the lowest level of police personnel, whether there is a structured training plan that law enforcement should follow or any official arrangement in place with academia and industry to support trainings on cybercrime. According to desk research, most of the trainings are 'informal and based on personal efforts and interests.'[118]

One participant acknowledged that a particular problem in educating police officers is the lack of specialized training on cybercrime (e.g.: intellectual property theft), financial crime (e.g.: money laundering), regardless of the level of government since the situation is the same at all state levels. In previous years, there have been more trainings organized by internationally funded projects and organizations, but only a small number of policemen were generally present, although all inspectors should attend such trainings. In 2019 some trainings were planned related to digital forensics and familiarising police officers with investigative/forensic techniques and computer crimes, including methods of executing cybercrime offenses that,

[112] Ministry of Interior of Government of Federation of Bosnia and Herzegovina. Internal Organization of the Federal Police Administration. Available at http://www.fbihvlada.gov.ba/english/ministarstva/unutrasnji_poslovi.php (Accessed 9/11/2018)
[113] Barakovic, S., & Husic, J. B. (2015) ''We Have Problems For Solutions": The State Of Cybersecurity In Bosnia and Herzegovina. Information & Security, 32(2), 1. (Accessed 9/11/2018)
[114] Agency for Education and Professional Training. https://www.aeptm.gov.ba/en/node/300 (Accessed 9/11/2018)
[115] Ibid.
[116] Ibid.
[117] Council of Europe. Octopus Cybercrime Community (2017) Bosnia and Herzegovina. Available at https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/bosnia-and-herzegovina?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view (Accessed 9/11/2018)
[118] Barakovic, S., & Husic, J. B. (2015) ''We Have Problems For Solutions": The State Of Cybersecurity In Bosnia and Herzegovina. Information & Security, 32(2), 1. (Accessed 9/11/2018)

due to the very nature of modern information technologies, are very different from traditional crimes and more sophisticated.
Also, it was highlighted that specialized trainings are often treated in police agencies as a 'rewarding trip'. When training is held abroad, it is very common that the management appoints high-ranking officials who would soon be retired or police officers who have achieved good results in their work, i.e. middle or top management.

At the entity level and in BD, the police academies within the ministries of interior are charged with the task of providing education for law enforcement personnel. Law enforcement representatives indicated that there is work being done towards keeping up with the development and equipment used, as well as with the trends in use of digital forensics equipment. Several participants stated that trainings on cybercrime offered by the police academies are basic and often organised jointly with international and regional bodies and bilateral donors, including Europol, OSCE, European Anti-Fraud Office (OLAF), French Embassy and the Council of Europe (CoE) through the iPROCEEDS project. It was pointed out that additional training is required in this area, as the provisions only cover basic aspects of cybercrime often resulting in unresolved legal cases (one of the participants mentioned a case involving the purchase of drugs online from a European country, where the authorities were unable to locate the perpetrator). In addition, law enforcement officials are also able to build their knowledge through additional courses on cybersecurity, but this is optional. Prosecutors and law enforcement officials are the first responders to cybercrime and need to work together and coordinate from the time of investigation to the interviewing of witnesses (see Dimension 2).

At the state level, participants indicated that there are no special courts for handling cybercrime cases, nor specialised mandatory trainings for judges and prosecutors on cybercrime. There is, however, some ad hoc training provided by international cybercrime specialists.

At the entity level and in BD, there are two trainings institutions that deliver education for judges and prosecutors: the Centre for Judicial and Prosecutorial Training of the Republic of Srpska and the Centre for Judicial and Prosecutorial Training of the Federation of BiH that are supervised by the High Judicial and Prosecutorial Council of BiH. The types of cybercrime trainings offered by these training institutions however, was unclear.

Several participants referenced that at the entity level and in BD a limited number of prosecutors and judges receive ad-hoc trainings sponsored by international and regional bodies such as the CoE through the iPROCEEDS project. With regards to the insufficient number of specialised investigators in the Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina, one participant referred to the limited financial and technical resources available. There was a general consensus among the participants that there is a need for more specialised prosecutors, judges and law enforcement personnel to deal with advanced cybercrime cases.

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

Stage: Formative

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

The authorities in Bosnia and Herzegovina have recognised the need to improve informal and formal cooperation mechanisms, both domestically and across borders.

The working-level cooperation between the judiciary, law enforcement, government and private sector was described by participants as informal and poor due to the different degrees of cooperation that exist between the law enforcement agencies and 68 ISPs at the state, entity level and in BD and the poor implementation of current legislations that are not sufficient.[119]

With regards to formal mechanisms of international cooperation the Ministry of Justice at the state level acts as the central coordinating body for mutual legal assistance in criminal matters.[120] Article 4 of the Law on Mutual Legal Assistance (MLA) in Criminal Matters (in force since 2009) states that MLA requests should go through the Ministry of Justice.[121]

> Article 4
> **Channels of Communication**
>
> Letters Rogatory requesting mutual legal assistance of the national judicial authorities shall be transmitted to foreign judicial authorities through the Ministry of Justice of Bosnia and Herzegovina. Requests for mutual assistance of foreign judicial authorities shall be transmitted to the national judicial authorities through the same channel.[122]

The law also refers to urgent cases where Interpol or Eurojust could act as a transmitting authority to receive MLA requests on the condition that a copy of request is shared with the Ministry of Justice.[123] Also, in exceptional cases the national judicial authorities can directly request MLA from a foreign judicial authority.[124] Based on desk research 'police authorities in BiH directly cooperate with police authorities of other countries, exchange information and

[119] Teleography (2018) https://www.telegeography.com/products/globalcomms/data/country-profiles/ee/bosnia-and-herzegovina/regulations.html
[120] Council of Europe. Octopus Cybercrime Community (2017) Bosnia and Herzegovina. Available at https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/bosnia-and-herzegovina?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view (Accessed 9/11/2018)
[121] Law on mutual legal assistance in criminal matters. Official Gazette of Bosnia and Herzegovina, No. 53/09.
[122] Ibid.
[123] Ibid.
[124] Ibid.

are able to participate in establishing joint investigative teams with other countries on the basis of the Law on MLA in Criminal Matters.'[125]

A 24/7 point of contact under the Directorate for Coordination of Police Bodies of BiH was established in accordance with the Budapest Convention that closely cooperates with INTERPOL.[126] Participants confirmed that the point of contact is able to tackle complex challenges and do verifications for proceedings and investigations as well.

At the entity level, the specialised police cybercrime unit of the Republic of Srpska has good working relationship with ISPs. Informal cooperation exists on a voluntary basis, since ISPs are not obliged to answer requests coming from law enforcement, only if criminal proceedings are initiated by the Prosecutor's Office and then a warrant is obtained by the police. The level of cooperation between ISPs and police structures were described as good.
However, the cooperation does have formal elements. For example, law enforcement can send a formal request when requesting data from ISPs. For instance, data can be requested from Facebook via police channels, however, the police cannot obtain the content of such profiles for which the police needs to address the request for international legal assistance. Participants added that there is a difference between requesting IP addresses or registration details. The latter has to go through the mutual legal assistance (MLA) process. With regards to police requests to foreign entities in relation to combatting online child pornography, participants described a good level of cooperation in the Republic of Srpska, the Federation of BiH and Brčko District.

BiH entered into an operational and strategic cooperation with Europol under the Temporary decision from 11 December 2013, which also covers computer crime.[127] The agreement states that BiH 'designates a national contact point to act as the central point of contact between Europol and other competent authorities of BiH.'[128] However, according to sources, BiH failed to establish the national contact point for cooperation with EUROPOL that 'could lead to the temporary suspension of the application of the Agreement.'[129]

At the state level, the Ministry of Security and CEPOL entered into a Working agreement in 2014 in order to enhance mutual cooperation on law enforcement training.[130] There is a designated point of contact for maintaining communication including the (state) Ministry of Security, the Ministry of the Internal Affairs of the Republic of Srpska, and the Ministry of the

[125] Barakovic, S., & Husic, J. B. (2015) ''We Have Problems For Solutions": The State Of Cybersecurity In Bosnia and Herzegovina. Information & Security, 32(2), 1. (Accessed 9/11/2018)
[126] Ministry of Security. Bureau for Cooperation with Interpol. Available at http://www.msb.gov.ba/onama/Default.aspx?id=1697&langTag=en-US (Accessed 14/11/2018)
[127] Ibid.
[128] Europol (2013) Agreement on operational and strategic cooperation between Bosnia and Herzegovina and Europol. Available at https://www.europol.europa.eu/sites/default/files/documents/operational_cooperation_agreement_with_bosnia_and_herzegovina.pdf (Accessed 14/11/2018)
[129] Delegation of the EU to BiH (2018) Local EU Statement on EUROPOL National Contact Point. Available at http://europa.ba/?p=59351 (Accessed 14/11/2018)
[130] CEPOL (2014) CEPOL signs Working Arrangement with Bosnia and Herzegovina. Available at https://www.cepol.europa.eu/media/news/cepol-signs-working-arrangement-bosnia-herzegovina (Accessed 14/11/2018)

Interior of the Federation of BiH.[131] BiH is also member of the Southeast European Law Enforcement Center (SELEC) with Border Police of Bosnia and Herzegovina acting as the national contact points for exchange of information.[132]

BiH is part of is part of iPROCEEDS – Cooperation on Cybercrime project under the IPA; earlier called Cybercrime@IPA. The iPROCEEDS project that started in 2016 covers seven countries in the region targetting money laundering connected with cybercrime and virtual currency. The Ministry of Security is leading the project, which will be finished by June 2019.

Among the various international cooperation channels available, the engagement with INTERPOL Sarajevo were described as an important channels to facilitate cross-border cooperation and information-sharing. INTERPOL Sarajevo has access to INTERPOL's secure communication linkage, I-24/7, which is a restricted-access Internet portal, providing police across the country instant and automated access to INTERPOL's criminal databases. The I-24/7 network is considered to be an informal cooperation because it is used only to share information for intelligence purposes, and not for evidence-gathering.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to BiH. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL FRAMEWORKS

R4.1 At the state level, consider full implementation of the regulations provided by the Budapest Convention on Cybercrime by updating and harmonising existing legislations. Similarly, at the entity level and in BD fully incorporate the principles of the Convention on Cybercrime in the relevant laws.

R4.2 At the state level, adopt new and harmonise its current legislation regarding cybersecurity in line with the EU's requirements published in the Cybersecurity Strategy of the EU and the NIS Directive.

[131] Council of Europe. Octopus Cybercrime Community (2017) Bosnia and Herzegovina. Available at https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/bosnia-and-herzegovina?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view (Accessed 9/11/2018)
[132] SELEC. Available at http://www.mfa.gov.rs/en/foreign-policy/eu/regional-initiatives/selec (Accessed 9/11/2018)

R4.3 At the state level, reorganise existing or establish corresponding bodies for the enforcement of legislation addressing cybersecurity and cybercrime.

R4.4 Consider setting up a periodic process of reviewing and enhancing BiH's laws relating to cyberspace to address the dynamics of cybersecurity threats (e.g.: hate speech online, cyber-bullying).

R4.5 Consider harmonising the Law on Personal Data Protection with the GDPR and ensure that legal mechanisms are in place which enable strategic decision-making. Determine the timeframe after which personal data are no longer required as evidence for investigation and must be deleted. Identify international and regional trends and good practices to inform the assessment and amendment of data protection laws and associated resource planning.

R4.6 At the state level, develop new legislative provisions through multi-stakeholder consultation processes on children's safety online, human rights online, consumer protection online and intellectual property online. Also adopt new legislative provisions for mandatory reporting of cyber security incidents.

R4.7 Dedicate resources to ensure full enforcement of existing and new cybersecurity, cybercrime and data protection laws and monitor implementation.

R4.8 Consider developing a platform for sharing electronic evidence between corresponding bodies both at the state and entity level.

R4.9 Foster research on human rights on Internet and ensure that measures are in place to exceed minimal baselines specified in international agreements.

CRIMINAL JUSTICE SYSTEM

R4.10 At the state level, consider establishing a specialised cybercrime unit in charge of investigations related to cybercrime and digital forensics under a corresponding body. Consider allocating the cybercrime unit under the Directorate for Coordination of Police Bodies of BiH within the Ministry of Security or creating a separate cybercrime unit directly under the Ministry of Security of BiH.

R4.11 At the state level, consider turning the newly established cybercrime unit into BiH's central point of contact to carry out cybercrime investigations both domestically and internationally. (Once the cybercrime unit is established at the state level under the Ministry of Security of BiH)

R4.12 At the state level, consider creating a Joint Cybercrime Action Taskforce (J-CAT) within the newly established cybercrime unit or a corresponding body. Similarly,

to J-CAT located at Europol's European Cybercrime Centre. The Taskforce would be a standing operational team of cyber liaison officers from the Federation of Bosnia and Herzegovina (FBiH), the Republic of Srpska (RS) and the Brčko District (BD) who would also act as a single point of contact of their corresponding entities (FBiH, RS, BD). All these officers would work from the same office to ensure that they can communicate with each other easily.

R4.13 At the state level, consider creating a National Cybercrime Laboratory/Digital Forensic Laboratory under the auspices of a corresponding body (e.g.: either under the national BiH CERT or Ministry of Security) in order to facilitate digital forensics. This will provide a platform to all law enforcement agencies to carry out cybercrime investigations at the state level.

R4.14 Invest in advanced investigative capabilities in order to allow for the investigation of complex cybercrime cases, supported by regular testing and training of investigators.

R4.15 Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody at all levels.

R4.16 At the state level, develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence through CEPOL, EC3 or other organisations. Consider making arrangements with academic or industry bodies to support the development and delivery of cybercrime training.

R4.17 At the state level, consider establishing institutional capacity building programmes for judges, prosecutors and police personnel from security agencies to acquire new ICT skills needed for cybercrime investigations (e.g. digital evidence gathering) and effective ways of enforcing cyber laws.

R4.18 Consider establishing standards for the training of law enforcement officers on cybercrime both at the state and entity level and in BD.

R4.19 Build a cadre of specialist prosecutors and judges to handle cybercrime cases and cases involving electronic evidence.

R4.20 Collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.21 Strengthen international cooperation to combat cybercrime based on existing legal assistance frameworks and enter further bilateral or international agreements.

R4.22 At the state level, consider setting up a Threat Intelligence Platform for real-time information sharing between the newly established cybercrime unit (under the Ministry of Security) and the newly established national BiH CERT.

R4.23 Allocate resources to support the exchange of information between public and private sectors domestically and to enhance the legislative framework and communication mechanisms.

R4.24 Enhance cooperation between the public sector and banks and other financial institutions regarding the sharing of incidents, in order to increase the level of cybersecurity awareness in BiH.

R4.25 At the state and entity level and in BD, facilitate and strengthen informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders, in particular ISPs.

DIMENSION 5 STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-up – Formative

The Law on Standardization of Bosnia and Herzegovina[133] and the Law on the Establishment of the Institute for Standardization of Bosnia and Herzegovina[134] have laid the foundation for promoting the voluntary implementation and use of BiH national standards, compliance with the rules of international and European standardization and the creation of the Institute for Standardization that acts as an independent state administrative organization for the activities in the field of standardization.[135] The role of the Institute includes: 1) raising awareness about importance and role of standardization through seminars; 2) promoting the

[133] Law on Standardization of Bosnia and Herzegovina. Official gazette of Bosnia and Herzegovina No. 19/01. Available at http://www.bas.gov.ba/images/upload/pdf/institut/zakoni/law_on_standardization.pdf (Accessed 14/12/2018)
[134] Law on the Establishment of the Institute for Standardization of Bosnia and Herzegovina. Official Gazette of Bosnia and Herzegovina" No. 44/04. Available at http://www.bas.gov.ba/images/upload/pdf/institut/zakoni/law_on_the_establishment_of_the_institute.pdf (Accessed 14/12/2018)
[135] Institute for Standardization. Available at http://www.bas.gov.ba/button_17.html (Accessed 14/12/2018)

development of standardization in order to fulfil the conditions for full membership in European Standards Organizations CEN and CENELEC; 3) inviting experts to participate in activities of international and European standards working bodies.[136]

However, the review found that participants from both the public and private sectors were not aware of any ICT standards promoted by the government, which suggests that at the state level there is no obligation to implement any national (or sector specific) ICT security standard. However, there is a Decision on Adoption of Information Security Management Policy in the Institutions of Bosnia and Herzegovina for the period 2017-2022, which presents the guidelines and standards for state level institutions in BiH. Participants added that International Organization for Standardization (ISO) certifications for private companies is not required by law and that the implementation of ICT standards and best practices is ad-hoc. According to one participant, the Agency for Identification Documents, Registers and Data Exchange of Bosnia and Herzegovina (IDDEEA) is the only agency that has implemented ISO 27001.

Nevertheless, one participant mentioned that some institutions have identified and implemented an international standard that specifies requirements for a quality management system (QMS) such as ISO 9001 adopted by the Central Bank of Bosnia and Herzegovina (BiH). According to sources, in April 2017, an intensive training was provided to employees on the implementation of ISO quality standards providing the necessary knowledge for ISO 9001 and its associated certificate.[137]

One of the main foreign policy objectives of BiH is to become a member of NATO, therefore the Ministry of Defence of BiH intends to comply with corresponding membership obligations. Since the country is part of the Membership Action Plan (MAP) – a formal step towards joining NATO – the MoD is required to comply with certain standards and procedures required by NATO. By 2021, the MoD intends to establish a secure cyber-environment for the Ministry's network and information systems. In addition, a participant noted that the MoD applies a series of standards that were approved by the ITU and other international organisations.

Similarly, at the state level there is no mandatory standard for any sector related to the procurement of hardware and software. Based on desk research, the 2004 Public Procurement Law was in force for ten full years before the adoption of the new BiH Law on Public Procurement in 2014 with the aim of harmonising national legislations with EU standards.[138] In 2011, the basis for e-Procurement has been established with the introduction of the GO-PROCURE information system that makes the submission of procurement procedure notices for publication faster and simpler.[139] One participant raised concerns regarding the clarity of the Law on Public Procurement. Participants acknowledged that 90% of the software used by the authorities is requested based on functionality and in some cases on performance; the security element is mostly ignored. In other words, during the software procurement process, cybersecurity is the last thing considered. One participant added that

[136] Ibid.
[137] Central Bank of Bosnia and Herzegovina (2017) Info CBBH. Available at https://www.cbbh.ba/Content/Read/610?lang=en (Accessed 14/12/2018)
[138] Law on Public Procurement (2014) Available at https://www.javnenabavke.gov.ba/legislativa/zakoni/Novi_ZJN_BiH_en.pdf (Accessed 14/12/2018)
[139] Public Procurement Strategy 2016-2020. Available at https://www.javnenabavke.gov.ba/vijesti/2016/Strategija_2016-2020_en.pdf (Accessed 14/12/2018)

in some organisations procurement of new software has not been performed in the past 10 years.

Focusing on standards in software development, there are different guidelines in place in both the public and the private sectors, but the extent to which these guidelines are related to cybersecurity is not clear. Participants' commentary indicated that at the state level there is no in-house software development within the institutions. Some participants noted that outsourcing IT solutions and services is very common in BiH. For instance, the MoD has hired a software company that works jointly with the Ministry on the development of the applicable software.

D 5.2 INTERNET INFRASTRUCTURE RESILIENCE

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Formative

Liberalization of the telecommunications market and development of high-speed broadband internet in BiH is dependent on the country's continuing integration with the EU and hence alignment of its regulatory and legislative frameworks with EU acquis for electronic communications. The country has lagged behind other Western Balkan countries on the level of alignment with the relevant EU acquis due to the governance bottlenecks, which in turn has had an impact on the competition in the telecommunications sector and the state of BiH's internet infrastructure.

As far as competition is concerned, there are three dominant telecom operators (with significant market shares) – BH Telecom, Telekom Srpske (m:tel), and HT Mostar. Two out of these three companies (BH Telecom and HT Mostar) are majority-owned by the entity government (FBiH). Telekom Srpske (m:tel) is majority-owned by Telekom Srbija, the dominant provider of fixed and mobile telephony in Serbia. Privately-owned Telemach is the third dominant telecom operator (ahead of HT Mostar) in the segment of fixed broadband connectivity. There are also a number of smaller internet service providers that are privately owned.

High wireline (fixed telephony) penetration is a good foundation for developing high-speed broadband connectivity. Desk research shows that in 2017 the country had 19.5% of fixed-telephony subscriptions, trailing only behind Serbia (39.1%), as far as the Western Balkan region is concerned[140]. According to the World Bank, this existing infrastructure -if well maintained- could be used for provision of the fixed broadband Internet access services via

[140] http://www.itu.int/net4/itu-d/idi/2017/index.html

DSL technology[141]. It is therefore unsurprisingly that xDSL is already the dominant type of access technology: 56.83% of the broadband subscribers in BiH rely on it (while cable subscribers constitute the second largest subscriber group, or 33.41 % of the total number of broadband Internet subscribers[142]). According to Communications Regulatory Agency (CRA), the broadband internet penetration subscriber base in Bosnia and Herzegovina reached 663,682 individuals as of 2017, thus translating to around 19% of broadband access in the country (the number of connections in relation to the total number of inhabitants).[143]

The same desk research shows that growth trajectory of wireless connections and of mobile broadband has been slower than in the Western Balkan region. As of mid-2018, the country's wireless penetration stood at ~99%, against the regional average of ~146%[144]. The country's mobile broadband population penetration (40%), registered as of 2016[145], was closer to the regional average of 55%, although it should be noted that BiH figures are based on the usage of 3G (third-generation wireless) services while figures of other countries also include the usage of 4G (fourth-generation wireless) services. There has been notable delay with the launch of 4G services in BiH, however the regulatory process to enable commercial 4G connectivity is finally underway, pending the decision of CRA. Well-developed wireless infrastructure is important to serve the rural and isolated areas of the country (65 percent of the population is rural) as an alternative to the fixed broadband networks.

Participants generally agreed that Internet services are reliable. However, it was not clear from the review whether the Ministries or the Government at the state level have their own infrastructure or not.

D 5.3 SOFTWARE QUALITY

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Start-up

Based on the review, there is no identified centrally managed catalogue of secure software platforms and applications at the state level in BiH. Policies for updating software products or

[141] http://documents.worldbank.org/curated/en/910521467992511665/pdf/101009-SCD-P151812-SecM2015-0318-IFC-SecM2015-0159-MIGA-SecM2015-0106-Box393245B-OUO-9.pdf
[142] Ibid.
[143] Communications Regulatory Agency. https://docs.rak.ba//documents/d4a46a61-18f8-45b2-afc5-b1784f009fe8.pdf
[144] Bosnia and Herzegovina. Global Comms Database (August 2018). TeleGeography.
[145] The year for which there are comparable data for the Western Balkan region from the national regulatory agencies.

monitoring the functionality of applications may exist but are not necessarily enforced or formulated – each organisation has its own requirements defined at the corporate level.

For instance, with regards to software quality, the government relies on large software companies such as Microsoft. Participants referred to the problem of updating and patching the software regularly, since most of the end-users are reluctant to manage updates and patches of software applications. Most of the participants agreed that the mind-set of the end-users should be changed and either trainings should be provided in order to highlight the reasons for the need to update the software regularly or procure better software. One suggested that this culture and mind-set might change if there were audits. Currently, there is no structured basic training available that would educate the users on these issues.

The MoD relies on only one manufacturer and software producer, because the change in software might complicate and damage the efficiency of communication channels. Cybersecurity is measured by conducting threat and vulnerability assessments (of the Ministry's information systems). There is also the option of paying for automatic software updates that makes the user morally obligated to use the most up-to-date software.

At the entity level, in the Republic of Srpska, there is a lack of 'hygiene' in the private sector but also in governmental sector – patching and updating the software is not well developed. This situation is similar at all levels of government in BiH.

D 5.4 TECHNICAL SECURITY CONTROLS

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Stage: Start-up

The adoption of technical security controls in the country varies across the sectors within the entities and organisations, but they are mostly ad hoc and not consistently deployed.

At the state level, there is no evidence of wider promotion of the use of technical security controls, nor incentives being offered to any sector for the use of up-to-date security controls. There is no evidence that ISPs are offering upstream controls or antimalware software as part of their services and whether they have policies in place for technical security control deployment. There is no evidence of a defined standard or good practices for up-to-date security controls, including backup and patching, in any sector.

There is no publicly available statistical data on the use and deployment of technical security controls by users, private or public sectors. One participant referred to the lack of ICT experts and financial means that is a significant problem within the public institutions. Another challenge is that cloud security is becoming more and more important whilst firewall is not enough anymore.

Participants suggested that the practice of patching operating systems and performing backups are widespread across sectors, but noted that there are no defined standards or good practices to guide these activities. Within the private sector there is a substantial level of technical security controls in place (such as firewalls, cloud storage, backups, guardians, access controls by smart cards (for authorized persons), video surveillance; every single entry is recorded; standard equipment UPS, antistatic controls) and prompted warnings for internal users, however it was not clear from the review if they are tested regularly. The Central Bank of Bosnia and Herzegovina (CBBH) offers general best-practice training at a basic level, however this is challenging since there are constantly new interfaces and new information; therefore CBBH relies on the users to also let the bank know if there is an incident.

At the entity level, the institutions in Republic of Srpska do not have firewall because of the reliance on third party security providers with regards to storage. Participants questioned the validity of technical security controls that were used five years ago.

D 5.5 CRYPTOGRAPHIC CONTROLS

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.

Stage: Formative

At the state level, cryptographic controls (Secure Sockets Layer (SSL); Virtual Private Network (VPN)) for protecting data at rest and in transit are recognised and deployed ad hoc by multiple stakeholders and within various sectors. Some participants mentioned that encryption is used for internal processes, but there are no certified employees. Within the banking sector, PGP encryption is also used for certain email communication and RMS protection tools to protect documents for internal purposes.

Participants noted that government does not pay sufficient attention to this area. Organisations using e-signatures are not certified. Some participants referred to adhering to the Law on the Protection of Personal Data regarding data at rest.

At the entity level, in the Republic of Srpska, the Department for Information Security within the Agency for Information Society was in charge of updating the list of algorithms that was made publicly available. The document titled 'Accredited Cryptographic Algorithms' contains a list of cryptographic algorithms accredited by the Information Security Unit for the institutions in the Republic of Srpska, in accordance with Art. 83 of the Rulebook on Security Information Standards.[146] The purpose of this document is to raise the level of information security in the institutions of the Republic of Srpska by standardizing the application of

[146] Agency for Information Society of the Republic of Srpska. 'Accredited Cryptographic Algorithms'. Available at https://oib.aidrs.org/sites/default/files/akreditovani-kripto-algoritmi.pdf (Accessed 21/03/2019)

cryptographic algorithms. To reduce the variety of algorithms used and avoid the use of algorithms that are considered unsuitable and can lead to information security disturbance and a list of permitted algorithms. The algorithms are divided into the following groups:

- Symmetric algorithms
- Stream Crypto algorithms (subgroups of symmetric algorithms)
- Asymmetric algorithms
- Algorithms for creating an electronic summary (hashing algorithms)
- Electronic Signature Algorithms

These five categories of cryptographic controls that were introduced by the law, however the implementation is only voluntary, although it might become mandatory in 2019. Currently, similar kinds of documents do not exist at other levels of government in BiH.

Within the MoD, NATO regulations with regards to classified data are very strict, there are only two types of data, national and NATO classified information and one participant noted that no mistakes are allowed.

At the state level, all institutions that have access to classified data have to comply with certain standards prescribed by the Sector for the Protection of Classified Information of the National Security Authority (NSA BiH) attached to the Ministry of Security of BiH and all systems have to be accredited. [147]

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-up

Participants from the public and private sectors noted that BiH does not currently produce cybersecurity technologies, but relies on international offerings.

No domestic market for cybercrime insurance products has yet been developed in the BiH. There was no discussion amongst participants that a market for insurance has been identified in BiH. Participants noted that their organisations had nothing to cover financial losses in the event of a serious cybersecurity incident.

[147] Sector for the Protection of Classified Information of the National Security Authority. Available at http://msb.gov.ba/onama/default.aspx?id=1685&langTag=en-US (Accessed 14/12/2018)

D 5.7 RESPONSIBLE DISCLOSURE

Stage: Start-up

This factor explores the establishment of a responsible-disclosure framework for the receipt and dissemination of vulnerability information across sectors and, if there is sufficient capacity, to continuously review and update this framework.

Currently, there is no policy in place for responsible information disclosure within the public or the private sector.

When asked about ways how users can report bugs and vulnerabilities, participants noted that currently there are no mandatory reporting requirements or mechanisms for cyber-incidents. One participant suggested that the new law that would be compliant with the GDPR could provide more provisions to oblige people to report incidents.

There was no discussion or evidence of the informal sharing of newly discovered or known vulnerabilities with a group who can further disseminate the information across sectors.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity Standards, Organisations, and Technologies, the following set of recommendations are provided to BiH. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1 At the state level, consider adopting a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors, including ICT security standards in procurement and software development. Consult with existing working groups and experts from all sectors, but in particular the banking sector, as well as audit companies and professional associations.

R5.2 Assign the Institute for Standardization of Bosnia and Herzegovina (BAS) responsible for the implementation, auditing and measurement of the success of standards across public and private sectors. Apply metrics to monitor compliance and establish periodic audits.

R5.3 Ensure that defined standards and guidance include: consideration of cybersecurity risks in all procurements of goods and services; secure

configuration of networks, devices, systems and applications; digital identify management, including authentication; and secure software development practices (including websites) where applicable.

R5.4 Identify a minimum set of controls for all governmental departments based on annual assessments and establish a controls-review to assess the effectiveness of the current controls and practices.

R5.5 Establish frequent training for IT employees within all governmental departments both at the state and entity level.

R5.6 Establish a framework to assess the effectiveness of standards for procurement and software development.

R5.7 Consider the implementation of international best practices in consultation with all relevant stakeholders and regulators.

R5.8 Establish mandatory requirements for the adherence to standards by appointing security officers who will be held responsible for the implementation of these standards.

INTERNET INFRASTRUCTURE RESILIENCE

R5.9 At the state level, assign an institution (e.g.: Communications Regulatory Agency) responsible for enhancing coordination and collaboration regarding the resilience of Internet infrastructure across the public and private sectors. Developing Internet infrastructure policy and assessing the deployment of technology and processes.

R5.10 Consider assigning the Communications Regulatory Agency to identify and map points of critical failure across the Internet infrastructure.

R5.11 Encourage ISPs to establish and publish service level agreements for services and report on service outages to the responsible agency.

R5.12 Define metrics for continuously measuring service reliability, collect data and publish reports to show trends.

R5.13 Identify, describe and revise assets, processes, roles, responsibilities and skills required for formally managing National infrastructure.

R5.14 Conduct regular assessments of the assets, processes, roles, responsibilities and skills required for managing Internet infrastructure to ensure that practices follow international standards, guidelines, good practices and address identified risks.

R5.15 Raise awareness with end users to enable them to identify services that have successfully implemented defined standards and good practices.

SOFTWARE QUALITY

R5.16 Establish or assign an institution responsible for developing software quality policy and assessing practices across sectors at the state level.

R5.17 In collaboration with public, critical infrastructure and private-sector partners, develop and revise a catalogue of applications and platforms that have been evaluated for software quality, functional requirements and security risks across sectors.

R5.18 Gather and assess evidence of software quality deficiencies regarding their impact on usability and performance.

R5.19 Address gaps in identified applications and platforms that have not been evaluated for software quality, functional requirements and security risks.

R5.20 Revise policies for assessing software for deficiencies to include guidance on measuring, evaluating and reporting the impact on usability and performance.

R5.21 Develop and revise policies and processes for regular updating and patching operating systems and applications for all government agencies to use.

R5.22 Promote across all sectors the policies and practices regarding: use of the catalogue of evaluated platforms and applications; updating and patching; and assessing software for deficiencies.

TECHNICAL SECURITY CONTROLS

R5.23 Adopt standards and good practices for selecting, configuring and deploying technical controls based on risk assessments for private and public sectors and end users.

R5.24 Encourage ISPs and banks to offer anti-malware and anti-virus services for clients and ensure that their effectiveness is monitored and assessed.

R5.25 Establish metrics for measuring the effectiveness of technical controls across the public domain.

R5.26 Develop processes for reasoning about the adoption of more technical controls based on risk assessment methodologies suitable for the public domain.

R5.27 Ensure that Network Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed in across the public sector.

R5.28 Consider raising awareness of security controls by promoting cybersecurity best practices for users, such as strong passwords, secure back-ups, and use of anti-malware on their devices.

R5.29 Designate an authority to be responsible for the strategic decisions on technical controls that will supervise end-to-end all networks and will promote the adoption of a unified framework for security controls.

R5.30 Keep technical security controls up-to-date within the public and private sector, monitor their effectiveness and review on a regular basis.

CRYPTOGRAPHIC CONTROLS

R5.31 Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines.

R5.32 Raise public awareness of secure communication services, such as encrypted/signed emails.

R5.33 Consider requiring all cloud services that share data to automatically encrypt data before it is uploaded. This will help the process of buying certain cloud services easier for companies.

R5.34 Use SSL/Transport Layer Security (TLS) connections to secure communications between government bodies and data centres.

R5.35 At the state level, establish or assign an institution to design a policy, aiming to assess the deployment of cryptographic controls, according to their objectives and priorities within the public and private sector.

R5.36 Consider incentives to promote the adoption of cryptographic controls across sectors.

CYBERSECURITY MARKETPLACE

R5.37 Foster collaboration with the private sector and academia regarding research and development of cybersecurity technological products.

R5.38 Encourage and support local initiatives in partnership with businesses that aim at developing innovative cybersecurity technology, applications, services and solutions.

R5.39 Promote sharing of information and best practices among organisations to explore potential cybercrime insurance coverage.

RESPONSIBLE DISCLOSURE

R5.40 At the state level, establish or assign an institution responsible for developing responsible disclosure policy and assessing the processes in place.

R5.41 In consultation with key sector stakeholders, develop and implement a responsible disclosure policy and processes for reporting bugs and vulnerabilities across sectors.

R5.42 In consultation with key sector stakeholders, develop and implement a policy and processes for sharing bug and vulnerability reports across sectors.

R5.43 Promote the adoption of the bug and vulnerability policies and processes across all sectors.

R5.44 Measure and evaluate the use of the bug and vulnerability policies and processes.

ADDITIONAL REFLECTIONS

Even though the duration of this review was shorter by half a day, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 28th country review that we have supported directly.

The review was conducted in cooperation with the World Bank and the dissemination of this report was carried out in cooperation with Global Cybersecurity Center for Development (GCCD) under Korea Internet Security Agency (KISA) of Republic of Korea. The financing came from Korea's Ministry of Strategy and Finance (MoSF) through the Korea-World Bank Group Partnership Facility (KWPF), which is administered by the World Bank.

Global Cyber Security Capacity Centre

Oxford Martin School, University of Oxford

Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,

United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435

Email: cybercapacity@oxfordmartin.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity