CYBERSECURITY CAPACITY REVIEW

Serbia

October 2019

CONTENTS

Document Administration 3
List of Abbreviations 4
EXECUTIVE SUMMARY 6

INTRODUCTION 13

Dimensions of Cybersecurity Capacity 16
Stages of Cybersecurity Capacity Maturity 17
Methodology - Measuring Maturity 18

CYBERSECURITY CONTEXT IN SERBIA 20

REVIEW REPORT 22

Overview 22

DIMENSION 1 CYBERSECURITY STRATEGY AND POLICY 23

D 1.1 National Cybersecurity Strategy 23
D 1.2 Incident Response 26
D 1.3 Critical Infrastructure (CI) Protection 30
D 1.4 Crisis Management 33
D 1.5 Cyber Defence 35
D 1.6 Communications Redundancy 38
Recommendations 39

DIMENSION 2 CYBERSECURITY CULTURE AND SOCIETY 46

D 2.1 Cybersecurity Mind-set 46
D 2.2 Trust and Confidence on the Internet 48
D 2.3 User Understanding of Personal Information Protection Online 49
D 2.4 Reporting Mechanisms 49
D 2.5 Media and Social Media 50
Recommendations 51

DIMENSION 3 CYBERSECURITY EDUCATION, TRAINING AND SKILLS 53

D 3.1 Awareness Raising 53
D 3.2 Framework for Education 55
D 3.3 Framework for Professional Training 58
Recommendations 59

DIMENSION 4 LEGAL AND REGULATORY FRAMEWORKS 64

D 4.1 Legal Frameworks 64
D 4.2 Criminal Justice System 71
D 4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime 74
Recommendations 75

DIMENSION 5 STANDARDS, ORGANISATIONS AND TECHNOLOGIES 78

D 5.1 Adherence to Standards 78
D 5.2 Internet Infrastructure Resilience 80
D 5.3 Software Quality 82
D 5.4 Technical Security Controls 82
D 5.5 Cryptographic Controls 83
D 5.6 Cybersecurity Marketplace 84
D 5.7 Responsible Disclosure 85
Recommendations 86

ADDITIONAL REFLECTIONS 90

DOCUMENT ADMINISTRATION

Lead researchers: Kenneth Herman (World Bank), Óscar Noé Ávila (World Bank)

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Professor Basie Von Solms, Dr Jamie Saunders, all members of the Technical Board of the Global Cyber Security Capacity Centre (GCSCC).

Approved by: Professor Michael Goldsmith (GCSCC)

Version	*Date*	*Notes*
1	*06/01/2020*	*First draft submitted to Technical Board*
2	*23/03/2020*	*Second draft submitted to MTTT*
3	*04/05/2020*	*Third draft submitted to MTTT*
4	*06/01/2020*	*Final draft submitted to WB*

LIST OF ABBREVIATIONS

BMU	Belgrade Metropolitan University
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CMU	Carnegie Mellon University
CoE	Council of Europe
DPO	Data Protection Officer
ENISA	European Network and Information Security Agency
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation (of the European Union)
GLACY+	Global Action on Cybercrime+
IAS	Informatics Association of Serbia
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technologies
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
KPA	Academy of Criminalistics and Police Studies (of Serbia)
LOJGA	Law on the Organisation and Jurisdiction of Government Authorities for Combating Cybercrime
LPDP	Law on Personal Data Protection
MEST	Ministry of Education, Science and Technological Development (of Serbia)
MIA	Military Intelligence Agency (of Serbia)
MoD	Ministry of Defence (of Serbia)
MoI	Ministry of Interior (of Serbia)
MSA	Military Security Agency (of Serbia)
MTTT	Ministry of Trade, Tourism and Telecommunications (of Serbia)
MUP CERT	CERT of the Ministry of Interior (of Serbia)
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology, US Department of Commerce
OSCE	Organisation for Security and Cooperation in Europe

PKI	Public Key Infrastructure
RATEL	Regulatory Agency for Electronic Communications and Postal Services (of Serbia)
RIPE	Réseaux IP Européens Network Coordination Centre
SAF	Serbian Armed Forces
SANS	(SysAdmin, Audit, Network and Security), an American internet security training company
SDIS	Strategy for the Development of Information Security 2017-2020
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNICEF	United Nations Children's Fund

EXECUTIVE SUMMARY

1. At the invitation of the Ministry of Trade, Tourism and Telecommunications, the World Bank undertook a review of the maturity of cybersecurity capacity in the Republic of Serbia. The objective of this review is to enable the country to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

2. Over the period of October 16-18, 2019 the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies, and the banking sector as well as international partners.

3. The consultations took place using the Cybersecurity Capacity Maturity Model (CMM), developed by the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre'), a part of the Oxford Martin School of the University of Oxford in the United Kingdom. The model 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*

4. Each dimension contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping 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]

5. Figure 1 below provides an overall representation of the cybersecurity capacity in Serbia 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 of the graphic 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* (accessed 25 February 2018).

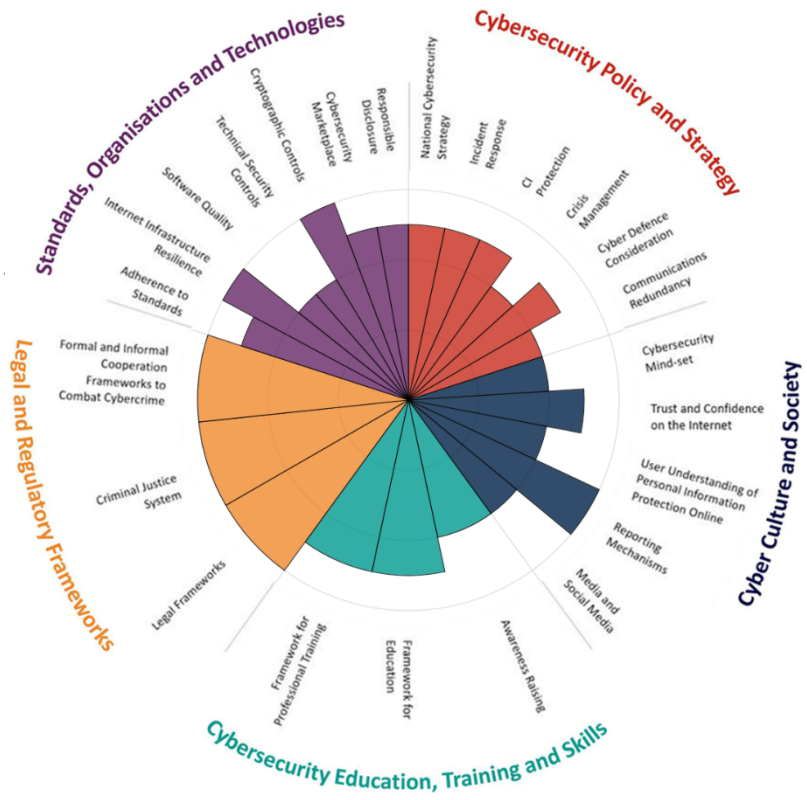

Figure 1: Overall representation of the cybersecurity capacity in Serbia

Cybersecurity Policy and Strategy

6. Overall, the Cybersecurity Policy and Strategy dimension of Serbia is assessed as Start-Up to Established.

7. Serbia adopted the Strategy for the Development of Information Security 2017-2020 (SDIS), which was officially published in May 2017 and its Action Plan 2018-2019 was not adopted until August 2018. When SDIS was drafted, multi-stakeholder consultation processes were followed, and observations fed back to coordinating agencies. International organisations (e.g. UNICEF, OSCE) also participated in the consultation sessions.

8. The 2018-2019 Action Plan has multiple projects and initiatives which were linked to national risks, priorities and objectives, as well as economic and social development plans. SDIS recognises that Ministry of Trade, Tourism and Telecommunications (MTTT) will monitor the SDIS implementation process. The SDIS and its Action Plan are being evaluated and outcomes will be published soon.

9. A coordinated national cybersecurity programme was established in Serbia. By law, MTTT is responsible for the ICT security of the country, including the implementation of the SDIS. Ministry of Interior (MoI) is responsible for cybercrime-related matters, including the implementation of the National Cybercrime Strategy. The “Body for the Coordination of Information Security Affairs” was also established by the Government but is essentially an advisory body.

10. The national CERT was established in 2017 with specified roles and responsibilities which are set out in the Law on Information Security. Regulatory Agency for Electronic Communications and Postal Services (RATEL) is responsible for managing the national CERT and MTTT supervises the CERT's work and performance.

11. The national CERT's scope is currently limited to incident handling and coordination (described by some interviewees as "Soft CERT"). The Law on Information Security allows the establishment of the following CERTs: the national CERT, the Government CERT, the CERT of Independent ICT Operators, and the Special CERTs. Even though there are different incident response mechanisms in Serbia, there persists a need to strengthen some specific areas within the incident response management process to reach a higher maturity level.

12. Serbia identified eight national critical sectors: energy, traffic, the supply of water and food, healthcare, finance, telecommunication and information technologies, protection of the environment, and the functioning of government entities. The Law on Information Security also sets out the list of Critical Information Infrastructure (CII) systems and networks which are known as ICT systems of Special Importance. This list of CII assets is being updated through an amendment to said law.

13. Various government agencies and ministries have taken multiple actions relating to crisis management, but not in a nationally coordinated manner. MoI has established robust policies, strategies, and laws as well as a coordination body regarding national disaster management (sector for emergency management). It was noted that cybersecurity was partially integrated into this specific structure, but it requires a national-level approach. MoD organises annual cyber drills ("Cyber Tesla"), but these simulations are not yet considered a national-level exercise due to the fact that not all relevant stakeholders are part of the drills while others just participate as observers.

14. The Ministry of Defence (MoD) is responsible for the cyber defence matters in Serbia. MoD has a good level of awareness and understanding concerning the need to enhance the cyber defence capacities of the nation. Serbia has not adopted a cyber defence strategy; however, the Government recently adopted a new National Security Strategy and a new National Defence Strategy (in 2019) which recognise the importance of addressing cybersecurity-related issues within their structures and it is likely that their action plans (which need to be developed) integrate some cyber-defence operations and activities.

15. Within the defence structure, there are multiples agencies which are related to cyber-defence operations and activities, such as the Serbian Armed Forces, the Military Security Agency, the Military Intelligence Agency, and the MoD CERT. This specific CERT is responsible for protecting the military ICT infrastructure from cyber threats.

16. Communication (Internet) redundancy as a broad concept has been addressed in Serbia. Internet network operators have been taken measures to enhance the communication redundancy capacity in the country. However, the Government agencies (mainly crisis management agencies, first responders and ISPs), have not convened to assess and identify the main gaps and overlaps in terms of emergency response assets communications and the roles and responsibilities of the authorities to maintain communications stability during a national crisis.

Cyber Culture and Society

17. The Cyber Culture and Society dimension was judged to range between the Formative and Established stages.

18. Cybersecurity awareness in Serbia can vary considerably, depending on the individual's environment. Many government employees are increasing their level of awareness, in part due to the growth of awareness training in the government. However, a cybersecurity mindset remains uneven across government entities. The importance of raising awareness amongst staff members and officials of local government entities was raised.

19. In the private sector the mindset depends on the industry and size of the company. The cybersecurity mindset is highest within the larger companies, particularly those with a more international presence, and most if not all the financial services and technology companies.

20. Within the general public, the consensus is that it varied considerably, but CMM participants indicated that there are indications that cybersecurity awareness and mindset were improving.

21. As with awareness, trust in the Internet is substantial, but not always based on a full understanding of the risks. There is a sense that most users accept what they see and do not critically assess what they see or receive online on a routine basis. E-government services are substantial and growing, with the government committed to these services. They are highly trusted, as are the growing number of e-commerce offerings, both from local as well as international companies.

22. The law on data protection is new and untested, and it is therefore difficult to assess its impact on the data protection environment, specifically the general public's understanding of personal information protection.

23. There are established mechanisms for reporting various types of cyber incidents, the most visible of these being the "Report an Incident" button on the home page of the national CERT. There is also a mechanism for reporting material on the Internet considered harmful to children.

24. In Serbia there appears to be only limited media coverage of cybersecurity topics, and only in an ad-hoc manner, although the national CERT has made efforts to educate members of the local press. There is very little social media coverage of cybersecurity issues.

Cybersecurity Education, Training and Skills

25. The assessment revealed that the *Cybersecurity Education, Training and Skills* capacity in Serbia ranges from the Formative to Established stages.

26. Serbia has several mechanisms operating that support cybersecurity awareness-raising for a broad range of stakeholders. The national CERT has a broad mandate related to cybersecurity awareness-raising, including training, while the Ministry of Trade, Tourism and Telecommunications maintains a campaign focused on online child protection. Several other entities also arrange awareness training for selected constituencies. There is no programme for executive awareness raising.

27. Serbia has recognised the need to enhance the ICT and cybersecurity education in primary and secondary schools and universities. At the school level, MEST developed mandatory IT training courses with basic cybersecurity components for children in primary and secondary schools. At the university level, MTTT recently mapped several relevant tertiary education institutions and recommended some special study programmes on information security in relevant universities. In general, the cybersecurity educational capacity in Serbia needs to be strengthened through a Government led comprehensive action plan.

28. In tertiary education, nine universities in Serbia offer accredited cybersecurity-related laboratories or courses within their undergraduate, graduate and post-graduate/doctoral degree programmes, such as computer security, e-business system security, information security, cryptography, secure software design, digital forensics, amongst others. Except for a master's degree programme, the existing courses do not provide a specialised degree in cybersecurity. A few universities occasionally offer short courses or seminars for non-specialists and have research and development projects in cybersecurity, but the impact of these courses and projects is relatively low. It is unclear whether qualification programmes for cybersecurity educators exists, although there is currently an adequate number of educators and academics to deliver the demand of existing courses.

29. Different sectors have recognised the need to enhance the professional training capacity in cybersecurity, but this requirement has not yet been documented at the national level. There is no initiative or project in that respect on the SDIS or its Action Plan. Training programmes in cybersecurity are offered for public and private sector employees, as well as for the general public. ICT professional certifications with some security modules or components are available in Serbia. Internationally accredited IT Security and Governance training and certification courses are offered in Serbia, such as *IT Security and Governance Certification Courses, Foundation Level IT Security and Governance Certification Courses* (Ethical Hacking Foundation Training and Certification and COBIT 5 Foundation Certification Training Course), *Intermediate Level IT Security and Governance Certification Courses* (CGEIT Course) *or Advanced Level IT Security and Governance Certification Courses* (CRISC Course, COBIT 5 Assessor Certification Training Course, COBIT 5 Implementation Certification Training Course).

Legal and Regulatory Frameworks

30. Legal and Regulatory capacities of Serbia were identified in Established stages of maturity.

31. Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in Serbia.

32. Serbia has an all-encompassing legal framework that deals explicitly with cybersecurity. Those laws address cybersecurity-related issues, such as personal data protection, cybercrime offences, IP protection of online services and products, child pornography, incident reporting obligations, protection of CII, security and integrity of electronic communication networks and services, handling of electronic documents in legal transactions, administrative matters, court and other procedures, amongst others.

33. In 2005, Serbia adopted the Law on the Organisation and Jurisdiction of Government Authorities for Combating Cybercrime (LOJGA) as part of the process of strengthening the legislative and institutional framework of the Judicial System. LOJGA established and defined the responsibilities and functions of the three main government bodies directly related to the investigation, prosecution and process of cybercrime cases in Serbia:

    i. the Cybercrime Unit,

    ii. the Special Prosecutor's Office, and

    iii. the Higher Court in Belgrade, which was designated as the competent court to try, among other cases, cybercrime offences for the entire country.

34. Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime. Serbia has established cooperation agreements with Interpol and Europol, as well as bilateral agreements with neighbouring countries and allies on cross-border information sharing and cybercrime-related matters. Moreover, informal relationships between government and criminal justice agencies as well as between ISPs and law enforcement exist, with clear communication channels resulting in the regular exchange of information on cybercrime cases.

Standards, Organisations, and Technologies

35. Serbia's capacity in *Standards, Organisations and Technologies* was assessed to range from the Formative to the Established stages.

36. ICT Security standards and good practices have been adopted by institutions in both the public and private sectors. The law on information security has been a driving force behind the adoption of standards as these are required for many critical systems. While the regulation does not prescribe any specific standard, many organizations in the government as well as the private sector, are adopting the ISO 27001 standard, and the measures of protection of that operators of ICT Systems of Special Importance are modelled on the ISO standard. In the private sector, the financial and telecommunications companies are most frequently adopting this standard, while companies in other industries are moving more towards internationally recognized frameworks and good practices.

37. Only a few participants indicated any special procedures related to the area of cybersecurity standards in procurement, and fewer still have adopted any software development standards.

38. Serbia has a robust, reliable and affordable internet infrastructure that has substantial redundancy and appears extremely well managed.

39. The environment for software quality can vary considerably depending on the institution and industry. The financial sector is leading in this area, with many firms reporting the existence of white-lists for software and a controlled installation and update environment, including rigorous testing of new software versions.

40. Up-to-date technical security controls are deployed in all sectors in Serbia, although the level of implementation can vary depending on the sector or size of the establishment. In the public sector, government entities interviewed noted it was

standard practice to apply many of these practices, while in the private sector these controls are mainly deployed by the larger institutions.

41. The use of cryptographic controls in Serbia is well understood, deployed and mandated through the Law on Information Security for the government and critical infrastructure operators. There is also use of these controls in the private sector for both data at rest and in transit.

42. Even though ICT as a business sector is growing, and the focus is mainly on software development for business applications, there are several Serbia-based companies creating cybersecurity products.

43. The Law on information security and the law on electronic communication both have mandatory disclosure requirements for operators and together provide a framework for disclosure of security incidents. A number of CERTs operate in the Serbian ecosystem, including a national CERT, a government CERT and many special CERTs.

Additional Reflections

44. The government of Serbia has clearly made cybersecurity a priority. The CMM team is thankful for the support of the Ministry of Trade, Tourism and Telecommunications as well as the active participation of all the stakeholder groups.

INTRODUCTION

45. At the invitation of the Ministry of Trade, Tourism and Telecommunications, the World Bank conducted a review of cybersecurity capacity of the Republic of Serbia. The objective of this review was to enable the government of Serbia to determine areas of capacity in which the government might strategically invest in order to improve their national cybersecurity posture.

46. Over the period October 16-18, 2019, stakeholders from the following sectors participated in a three-day consultation process:

- Public sector entities
  Ministry of Trade, Tourism and Telecommunication (Ministarstvo trgovine, turizma i telekomunikacija)
  Ministry of Education, Science and Technology Development (Ministarstvo prosvete nauke i tehnološkog razvoja)
  Ministry of Justice (Ministarstvo pravde)
  Ministry of Finance (Ministarstvo finansija)
  Ministry of Commerce (Ministarstvo privrede)
  Ministry of Foreign Affairs (Ministarstvo spoljnih poslova)
  Ministry of Construction, Transport and Infrastructure (Ministarstvo gradjevinarstva, saobraćaja I infrastructure)
  Ministry of Health (Ministarstvo zdravlja)
  CERT of Ministry of Interior (Ministarstvo unutrašnjih poslova, Centar za reagovanje na napade na informacioni sistem (CERT))
  CERT of Republic Public Bodies (Kancelarija za informacione tehnologije I elektronsku pravu)
  Commissioner for information of public importance and personal data protection (Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti)
  Military Security Agency (Vojnobezbednosne agencija)
  National CERT (Regulatorna agencija za elektronske komunikacije I poštanske usluge, Nacionalni CERT)
  National Contact Centre for Children's Safety (Nacionalni kontakt centar za bezbednost dece na internet)
  National Employment Office (Nacionalna služba za zapošljavanje)
  Office of the National Security Council and Classified Information Protection (Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka)
  Ombudsman of Serbia Protector of Citizens (Zaštitnik građana Ombudsman)
  RATEL (Regulatorna agencija za elektronske komunikacije I poštanske usluge)
  Secretariat-General of the Government (Generalni sekretarijat Vlade)
  Security Information Agency (Bezbednosno-informativna agencija)
  The Intellectual Property of Republic of Serbia (Zavod za intelektualnu svojinu)

- Criminal justice sector
  The Republic Public Prosecutor (Republičko javno tužilaštvo)

Special Prosecution Office for Cybercrime (Posebno tužilaštvo za visokotehnološki criminal)
High Court in Belgrade (Viši sud u Beogradu)
Department for Cybercrime of Ministry of Interior / Department for High Technology Crime (Ministarstvo unutrašnjih poslova, Odeljenje za visokotehnološki criminal)
Police IT forensics support Unit (Direkcija policije, Nacionalni centar za kriminalističku forenziku, Odeljenje za elektronska i informatička forenzička veštačenja)

- Finance sector
  National Bank of Serbia (Narodna banka Srbije)
  Administration for the Prevention of Money Laundering (Ministarstvo finansija, Uprava za sprečavanje pranja novca)
  Association of Serbian Banks (Udruženje banaka Srbije)
  Banca Intesa (Banca Intesa akcionarsko društvo Beograd (Novi Beograd))
  Komercijalna banka (Komercijalna Banka AD Beograd)
  AIK banka (Agroindustrijsko Komercijalna banka AIK banka akcionarsko društvo, Beograd)
  Banka Poštanska Štedionica (Banka Poštanska Štedionica)
  NLB Banka (NLB banka AD Beograd)
  Srpska Banka (Srpska Banka AD Beograd (Savski Venac))

- Private Sector
  Unicom-Systems d.o.o. – Uni-CERT (Unicom-Systems d.o.o. – Uni-CERT)
  RNIDS (Fondacija ''Registar nacionalnog domena Srbije'')
  Serbian Open eXchange (Serbian Open eXchange)
  Telekom Srbija (Telekom Srbija)
  Naftna industrija Srbije (NIS)
  Electric Power Industry of Serbia (Elektroprivreda Srbije (EPS))
  Telekom (Telekom Srbija)
  NELT (Nelt Co d.o.o Beograd)
  Microsoft (Microsoft Software d.o.o.)
  CISCO (CISCO Srbija)
  IBM Serbia
  NALED (NALED)

- Critical infrastructure owners
  National Health Insurance Fund (RFZO)
  Energy Agency of Republic of Serbia (Agencija za energetiku)
  Electric Power Industry of Serbia (EPS) (Elektroprivreda Srbije)
  Elektromreža Srbije (EMS) (Elektromreža Srbije (EMS))
  Naftna industrija Srbije (NIS)
  Srbija gas (JP “SRBIJAGAS“, Novi Sad)
  JSC Serbian Railways (“ŽELEZNICE SRBIJE“ ad)
  PE Roads of Serbia (JP "Putevi Srbije")
  Port Governance Agency (Agencija za upravljanje lukama)

- Academia
  School of Electrical Engineering Belgrade (Elektrotehnički fakultet Beograd)
  Faculty of Organizational Sciences Belgrade (FON)

Academy of Criminalistics and Police Studies (Kriminalističko-policijska akademija)
Faculty of Security Studies Beograd (Fakultet bezbednosti Univerzitet u Beogradu)
SHARE Foundation (SHARE Fondacija)
Local ISACA Chapter (Udruženje ISACA Beograd)
DIPLO Foundation
Child Rights Centre (Centar za prava deteta)

- International community
  UNOPS (UNOPS Serbia Operations Centre)
  USA (Ambasada Sjedinjenih Američkih Država)
  UK (Ambasada Velike Britanije)
  Delegation of EU (Delegacija Evropske Unije u Srbiji)

DIMENSIONS OF CYBERSECURITY CAPACITY

47. Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM)[2] which is composed of five distinct *dimensions* of cybersecurity capacity.

48. 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 Cybercrime
Dimension 5 Standards, Organisations, and Technologies	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

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

STAGES OF CYBERSECURITY CAPACITY MATURITY

49. Each dimension contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping 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 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.

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

METHODOLOGY - MEASURING MATURITY

51. 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.

52. 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.

53. The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[3] 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.[4] It is this interaction and tension that offers advantage over other 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.[5]

54. 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.[6]The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[7]

55. 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

[3] Relevant publications: Williams, M. (2003). *Making Sense of Social Research*. Sage Publications: London; Knodel, J. (1993). "The Design and Analysis of Focus Group Studies: A Practical Approach". in *Successful focus groups: Advancing the state of the art*. Morgan, D. L. (Ed.). SAGE Publications: Thousand Oaks, CA; Krueger, R.A. and Casey, M.A. (2009). *Focus Groups: A Practical Guide for Applied Research*. Sage Publications: London.

[4] Relevant publications: Kitzinger, J. (1994)."The Methodology of Focus Groups: The Importance of Interaction between Research Participants. "*Sociology of Health & Illness*, 16(1). Available at https://doi.org/10.1111/1467-9566.ep11347023 (accessed 25 February 2018); Kitzinger, J. (1995). "Qualitative Research: Introducing Focus Groups". *British Medical Journal*, 311(7000). Available at https://doi.org/10.1136/bmj.311.7000.299 (accessed 25 February 2018); Fern, E.F. (1982)."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*, 19(1). Available at https://doi.org/10.1177%2F002224378201900101 (accessed 25 February 2018).

[5] Kitzinger, J. (1995).

[6] Krippendorff, K. (2004).*Content Analysis: An Introduction to its Methodology*. Sage Publications: Thousand Oaks, CA; Hsieh, H.F. and Shannon, S.E. (2005). "Three Approaches to Qualitative Content Analysis*." Qualitative Health Research*, 15(9). Available at https://journals.sagepub.com/doi/pdf/10.1177/1049732305276687 (accessed 25 February 2018); Neuendorf, K.A. (2002). *The Content Analysis Guidebook*. Sage Publications: Thousand Oaks, CA.

[7] Fern, E.F. (1982).

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.[8] 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.[9] Dey explains that this process categorises data as "belonging together".[10]

56. 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]

57. 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 the data collected by the Centre, which is a mixture of deductive and inductive approaches.

58. 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 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 the Centre's recommendations.

59. 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.

60. 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.

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

[8] *Elo, S. and Kyngäs, H. (2008). "The Qualitative Content Analysis Process."Journal of Advanced Nursing, 62(1). Available at* ***https://doi.org/10.1111/j.1365-2648.2007.04569.x*** *(accessed 25 February 2018); H.F. and Shannon, S.E. (2005).*

[9] Downe-Wamboldt, B. (1992)."Content Analysis: Method, Applications, and Issues."*Health Care for Women International*, 13(3). Available at https://doi.org/10.1080/07399339209516006 (accessed 25 February 2018).

[10] Dey, I. (1993).*Qualitative Data Analysis: A User-friendly Guide for Social Scientists*. Routledge: London.

CYBERSECURITY CONTEXT IN SERBIA

62. The Republic of Serbia, a landlocked country in south-eastern Europe, has a population of just over 7 million, evenly distributed in an area of just over 77,000 square kilometres[11]. According to ITU statistics, the percentage of individuals using the Internet in Serbia has almost doubled in the past 10 years, going from 38.1% in 2009 to 73.4% in 2019[12]. Serbia places as 55 (out of 176 countries) on the 2017 International Telecommunications Union (ITU) Global ICT Development Index[13]. According to the World Economic Forum's Global Information Technology report for 2016, Serbia ranked 75th out of 139 countries on their Network Readiness Index[14]. Interestingly, Serbia ranked 48th on the Readiness Subindex, with relatively high scores in the affordability and Infrastructure components at 56 and 45 (out of 139), respectively. The statistics from the WEF report shows that Serbia has a mobile subscription rate of 122% of the population, with a mobile broadband rate of 66% of the population and just over half of the households with internet access.

63. During the past 10 years, the government of Serbia has been pursuing a digital agenda, manifested through the development of a number of strategies. Many of these can be found on the government's strategy web page (http://www.gs.gov.rs/english/strategije-vs.html). Notable among these are a strategy for the development of the "information society"[15], as well as several others focused on telecommunications. All of these, and perhaps others, make reference to "security" of the technology or telecommunications environments.

64. It was not until the country adopted the "Law on Information Security"[16] in 2016 that cybersecurity came into sharper focus. This law established the guidelines and mechanisms that the country would use to create a more cyber-secure environment. This includes the creation of the national CERT, which operates under the authority of the telecommunications regulator, RATEL. The law also defines the scope and the protection measures for operating what it calls "ICT Systems of Special Importance". These are systems operated by public sector bodies, systems that store sensitive personal data, and systems managed by critical infrastructure operators. The law also prescribes overall reporting mechanisms and the protections that these systems should adhere to.

65. Subsequent to the passage of the law, in 2017 the government also adopted the "Strategy for the Development of Information Security in the Republic of Serbia for

[11] https://www.cia.gov/library/publications/the-world-factbook/geos/ri.html
[12] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[13] https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017rank-tab
[14] http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf
[15] http://www.srbija.gov.rs/extfile/sr/135791/strategija_razvoja_informacionog_drustva0288_cyr.zip
[16] Law on Information Security. *"Official Gazette of the Republic of Serbia"*, no. 6/2016.

the period 2017-2020", which identifies, *inter alia*, the background, regulatory framework, principles information security development and priority areas and strategic directions for the country in the cybersecurity area. This was followed by an action plan, published in August of 2018.

66. The development of the information security law and strategy emerged through a multistakeholder consultative process in 2014 and 2015[17]. This initiative, called the "Petnica Group", named after the location where the meetings were held, informally brought together specialists from the public, private and civil society sectors to discuss the direction of cybersecurity in the Republic of Serbia, and was supported by the Organization for Security and Cooperation in Europe (OSCE), Diplo Foundation and DCAF - Geneva Centre for Security Sector Governance.

[17]https://mtt.gov.rs/en/releases-and-announcements/towards-a-national-cyber-security-strategy-in-serbia-the-missing-elements-seminar-opened-at-petnica-research-station/

REVIEW REPORT

OVERVIEW

67. This section provides an overall representation of the cybersecurity capacity in Serbia. 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 of the graphic and 'dynamic' at the perimeter.

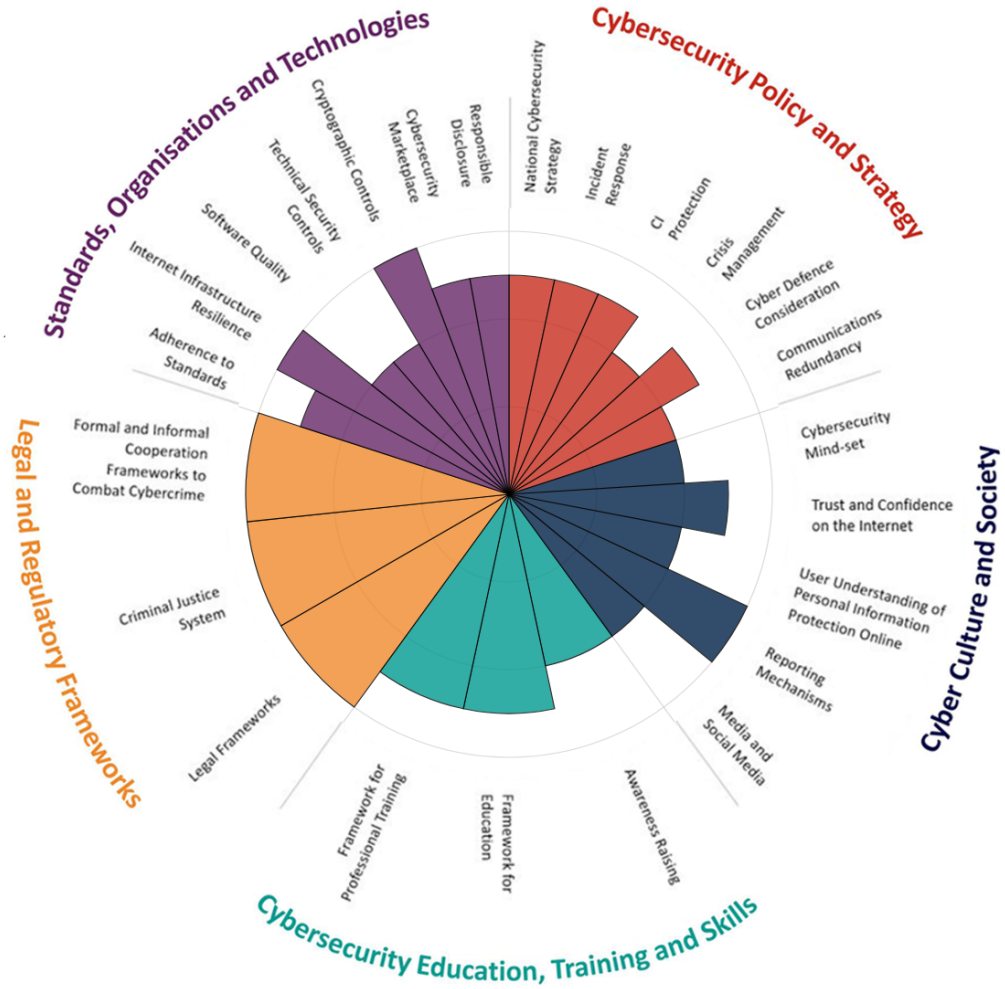

Figure 2: Overall representation of the cybersecurity capacity in Serbia

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

68. The factors in Dimension 1 gauge Serbia'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: Formative to Established

69. The Republic of Serbia adopted the Strategy for the Development of Information Security 2017-2020 (SDIS), which was officially published in May 2017. However, its Action Plan 2018-2019 was not adopted until August 2018. It was noted that SDIS clearly sets out a number of guiding principles for the development of information security in Serbia, as well as some priority areas that include the security of information and communication systems, security of citizens when using technology, and fight against cybercrime and information security of the country.[18]

70. During the SDIS drafting process, multi-stakeholder consultation processes were followed, and comments and observations were submitted to both MTTT (as the lead ministry) and established working groups. It was also noted that stakeholders from government, private sector, civil society and other relevant sectors participated in the drafting and consultation processes. Some relevant international organisations (e.g.

[18] https://www.osce.org/mission-to-serbia/404255?download=true

UNICEF, OSCE, among others) also joined and participated in the consultation sessions. It was noted that non-governmental actors do not have any participation in the implementation process of the current SDIS Action Plan. Despite the above, the Action Plan, in its section 1.5., establishes a number of activities related to the cooperation between the public and private sector.[19]

71. It was noted that the SDIS recognises that the development and improvement of the information security matters in Serbia should be achieved through the enhancement of the legal and institutional framework, protection of critical information infrastructures, and the fight against cybercrime and scientific research. To achieve those general objectives, SDIS identified the following five priority areas and fifteen strategic objectives:

1-) Security of information and communication systems:

- Prevention and protection by sharing information, monitoring current risks and raising awareness
- Security of ICT systems in business entities and security of e-commerce
- Security of ICT Systems of Special Importance
- Security of classified data in ICT systems
- Cooperation between public and private sector organisations in the field of information security

2-) Information security of citizens:

- Children's safety on the Internet
- Protection of privacy and protection against abuse in the use of ICT
- Information security in the education system

3-) Fight against cybercrime:

- Improving the mechanisms for detecting cybercrime and prosecuting the perpetrators
- Raising awareness of the dangers of cybercrime
- Promotion of international cooperation in the fight against cybercrime

4-) Information security of the country

- Information security system of importance for national security
- Development of scientific, technological and industrial capacities necessary for protection of information security of Serbia
- Building military defence system capacities to defend the country against cyber attacks
- Building security and intelligence capacities in the field of information security

5-) International Cooperation

[19] https://mtt.gov.rs/download/Action plan 2018-19 for implementation of the Strategy Information Security in Republic of Serbia.pdf

72. The 2018-2019 Action Plan breaks down those strategic objectives into multiple projects and initiatives that are linked to national risks, priorities and objectives, as well as economic and social development plans.

73. SDIS does not provide any review procedures, but it recognises that the implementation process will be monitored by MTTT. Some government stakeholders pointed out that MTTT, in collaboration with other government agencies, is currently evaluating, based on collected metrics, the performance of the existing projects and initiatives set in the Action Plan. MTTT expects that outcomes will be published soon. It was noted that this evaluation will help them to ascertain what needs to be improved and the next steps for both the preparation of the 2020 Action Plan and eventually the development of a new national cybersecurity strategy.

74. It was noted that a coordinated national cybersecurity programme was established in Serbia. Although SDIS does not provide any guidelines in that respect, the Law on Information Security sets out that MTTT is responsible for the ICT security of the country (article 4), including the implementation of the SDIS. However, cybercrime-related matters fall within the competence of the MoI. The latter is also leading the implementation of the National Cybercrime Strategy. This strategy also sets out a governance structure for cybercrime-related matters which is detailed in the Law on the Organization and Jurisdiction of Government Authorities Fighting against High Technological Crimes (2005). Both governance structures are part of the whole national cybersecurity programme.

75. The Law on Information Security also created the "Body for the Coordination of Information Security Affairs", which was established by the Government and is, in essence, an advisory body. This coordination body is composed of representatives of ministries responsible for information security, defence, internal affairs, foreign affairs, justices, security services, Office of the National Security Council and Classified Information Protection, General Secretariat of the Government, and Government CERT and national CERT (article 5). The Body for Coordination is also entitled to create professional working groups to support them in specific areas which require some level of specialisation. Those working groups could have representatives from public sector bodies, academia, economic and non-government sectors (article 5).

76. It was also noted that each government agency or ministry has an independent budget line for its internal cybersecurity issues, which includes some funds for the implementation of the SDIS projects and initiatives that they manage. Some government stakeholders pointed out that the budget for the implementation of the SDIS should be revisited and strengthened.

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: Formative to Established

77. In Serbia, the national CERT (Computer Emergency Response Team) was established in 2017[20] with specified roles and responsibilities which are set out in the Law on Information Security (article 14 and 15).[21][22]

78. This law provides the legal mandate for *the National Centre for the Prevention of Security Risks in ICT Systems* (hereinafter the "national CERT"), which is responsible for performing the tasks of coordinating the prevention and protection against security risks in ICT systems at the national level (article 14). The national CERT also helps to raise awareness on issues of network and information security and provides advice and alerts to the general public (article 15).[23]

79. This law also states that the telecom regulator, RATEL, is responsible for the activities of the national CERT (article 14) and that MTTT, as the Competent Authority, is responsible for supervising the work and performance of the national CERT. MTTT is entitled to inspect, at least once a year, whether the national CERT has adequate resources, performs the specified functions (article 15), and manages the established processes to respond to security incidents (article 16). It was also noted that the last inspection was conducted in November 2019 in accordance with the Inspection Plan of 2019.[24] Also, the national CERT has to submit quarterly reports to MTTT on undertaken activities -according to article 15.7 of the Law on Information Security.

80. It was noted that this CERT has a national reach, which covers critical infrastructures, operators of ICT Systems of Special Importance, private sector organisations and the general public, amongst others. Even though the national CERT works closely with the telecom operators, and even though the national CERT is based in RATEL (the telecom regulator), according to the participants the telecom operators do not receive any preferential treatment from the national CERT over other constituents.

81. Some government stakeholders pointed out that the national CERT currently has six staff members: four IT security experts, one lawyer, and one expert in promotion and awareness-raising matters. Those IT experts are highly trained both locally but mostly abroad. They approved the TRANSITS-I and TRANSITS-II courses and the Cybersec First Responder training, among other courses and certifications. There is a well-planned

[20] https://www.trusted-introducer.org/directory/teams/srb-cert.html

[21] https://www.cert.rs/en

[22] Articles 14, 15 and 16 of the Law on Information Security

[23] https://www.cert.rs/files/shares/RFC2350%20SRB-CERT.pdf

[24] https://mtt.gov.rs/download/Plan%20inspekcijskog%20nadzora%202019%20-%20izmene%20i%20dopune.pdf

and budgeted training programme for the next four years. The national CERT depends financially on RATEL to operate.

82. As part of its core functions which are detailed in article 15, the national CERT monitors and maintains a registry of all reported cyber incidents at the national level. On its website, the national CERT offers two means to report cyber incidents: via an online incident reporting form (https://www.cert.rs/en/prijava.html and https://mtt.gov.rs/prijava-incidenata-u-oib/?script=cir) and via email address (info at cert.rs).[25] It was also stated that there is a mobile number which is available 24/7 for incident reporting. Only in 2019 (up to October 17th) the national CERT recorded a total of 31 incidents; however, the reporting culture in the general public, including private sector organisations, has to be strengthened. As part of its awareness-raising functions, the national CERT also promotes certain information during workshops, such as the information on their mandate, on the current cybersecurity landscape in the country, and the information on the means available for incident reporting 24/7.

83. Based on international good practices, the national CERT has defined and documented internal incident response procedures (not publicly available) to manage its core function adequately. When a cyber incident is reported, the subject cyber incident passes through different analysis stages until its resolution. It was noted that those procedures are not audited by third parties but are regularly updated.

84. Some government stakeholders pointed out the national CERT is not currently conducting digital forensic (currently not part of its competences) and intelligence threat analysis, but they plan to do so in the future. Despite the above, it was noted that the national CERT's staff has been trained in digital forensics matters and these skills are currently used only for incident analysis. It was noted that by law the national CERT's scope is currently limited to incidents handling and coordination (described by some interviewees as "Soft CERT"). It was also noted that digital forensic analysis for cybercrime purposes is conducted by the pertinent unit/laboratory within the MoI.

85. Concerning incident reporting before the national CERT, the operators of ICT systems of Special Importance (which includes public and private operators) are currently obliged to report cyber incidents to the national CERT through the single system[26]. Now with the amendments to the Law on Information Security and new regulations on incident reporting procedures,[27] both the National Bank and RATEL are also obliged to report through the single system all the reported cyber incidents from their community members (financial institutions and telecom operators, respectively). Concerning private sector organisations (non CII operators), they are not obliged to report by law; however, participants pointed out that they understand that incident reporting is a good practice that works in their benefit and the rest of the ecosystem.

86. It was noted that other domestic CERTs also share information with the national CERT and are in constant communication (regular meetings). It was noted that actors within

[25] https://www.cert.rs/files/shares/RFC2350%20SRB-CERT.pdf

[26] Single system for incidents reporting is a platform which is set up in both the MTTT's portal and the national CERT's portal but it is managed by the MTTT. There, a variety of public and private organisations can report cyber incidents. The Law on Information Security, in its article 2.11.a, defines the single system as "…an information system inspecting incident data in ICT systems of significant importance that may have a significant influence on distribution of information security."

[27] https://mtt.gov.rs/en/download/r2.pdf

the Serbian criminal justice system, mainly law enforcement agencies, are often in communication with the national CERT.

87. In general terms, the national CERT has developed robust domestic and international cooperation networks. For instance, the national CERT was recently accredited by Trusted Introducer (August 2019).[28] It is part of the FIRST Fellowship Programme (working towards the membership), and ENISA – Article 13a Expert Group (2009/14/EU Directive). The national CERT works closely with the ITU programme which aims to improve the national CERT's capacities and also participates in the SEI/CMU table-top exercises.[29] It was noted that the national CERT is the point of contact in Serbia for technical matters only (e.g. OSCE's CBM 8). The national CERT's staff members has participated in multiple cyber drills locally and internationally, including the Cyber Tesla drills.

88. It was noted that the national CERT has multiple challenges, but all participants agreed that the main ones are related to human resources. Staff hiring within the public sector is forbidden by law due to certain budget restrictions, so new hiring is not possible until this restriction is lifted. Wages within the public sector are relatively low compared with the wages in the private sector, so retaining skilled people has become a significant issue. Even though the staff of the national CERT is constantly trained, it was noted that the delivery of capacity building needs to be strengthened.

89. In Serbia, the Law on Information Security allows the establishment of the following CERTs:

    1. ***the national CERT:*** (described in this section). It was noted that the national CERT is basically a hub for cyber incident coordination. Some government stakeholders pointed out that the incident response management function of the national CERT ranks 70/100, so there is still space for improvement. It was noted that the main difference between the national CERT and the Government CERT is that the former is an advisory body for the owners of the ICT systems and the latter owns the ICT systems. The national CERT does not have the executive powers.

    2. ***the Government CERT***: It operates under the aegis of the Office for IT and e-Government.[30] This CERT has operated for more than a decade, but it was formally created by the Law on Information Security in 2016. This incident response team protects the ICT infrastructure of the government agencies, ministries and municipalities (except for the independent ICT operators mentioned below).

    3. ***the CERT of Independent ICT Operators:*** the following ministries and agencies are obliged by law to protect their own ICT infrastructure and therefore establish their own CERT. They are not obliged to report cyber incidents to other government authorities, including the national CERT; however, they shall mutually exchange information about incidents, as well as with the national CERT and with the CERT of public authorities, and, if necessary, with other organisations (article 19 Law on Information Security).

[28] https://www.trusted-introducer.org/directory/teams/srb-cert.html

[29] https://mkd-cirt.mk/wp-content/uploads/2019/04/2019Ohrid_6.1.-Jelica-Vujadinovic-SRB-CERT-Nacionalni-CERT-Ohrid-2019-v1.pdf

[30] https://www.ite.gov.rs/tekst/88/cert.php

- ***CERT of the Ministry of Defence*** (in operation). Further information will be provided in section D.1.5.
- ***CERT of the Ministry of Interior*** (in operation). It was noted that this particular CERT has sufficient human, technological and financial resources to handle the entire incident response management process. This CERT, known as MUP CERT, was established in 2015 and was accredited by Trusted Introducer in 2018.[31]
- ***CERT of the Ministry of Foreign Affairs*** (in operation). No information was provided during the review sessions.
- ***CERT of the Intelligence Service Agencies*** *(*in operation*).* No information was provided during the review sessions.

4. ***the Special CERTs***: By law the national CERT is obliged to register the Special CERTs in Serbia. Currently, there are nine registered special CERTs.[32] It was noted that most of these Special CERTs are services providers. This type of CERTs is regulated by article 17 of the Law on Information Security.

90. It was noted that *the Government CERT*, *the CERT of Independent ICT Operators,* and *the Special CERTs* are entirely independent; hence, they can decide when and how to collaborate with other CERTs in Serbia. With the recent amendments to the Law on Information Security (passed late in 2019), those CERTs shall participate in planning and coordination meetings at least three times a year (article 15a of the Law on Information Security).

91. Serbia has developed an incident response management structure within the public sector which allows ministries and other government agencies to have adequate capacity to identify and respond to cyber incidents. Concerning private sector organisations, the national CERT and the Special CERTs are capable to assist them (including CII operators) in the incident handling process. Even though there are different incident response management bodies in Serbia, it was noted that those bodies need, especially the national CERT, to strengthen some specific areas within the incident management process to reach out to a higher maturity level. In the case of the national CERT, the CMM review team recommends reviewing the scope of its legal mandate, resourcing, operating procedures and performance.

[31] https://www.trusted-introducer.org/directory/teams/mup-cert.html
[32] https://www.cert.rs/en/evidencija-certova.html

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

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.

Stage: Formative to Established

92. In 2018, Serbia adopted the Law on Critical Infrastructures, which identified the following **eight national critical sectors**: energy, traffic, the supply of water and food, healthcare, finance, telecommunication and information technologies, protection of the environment, and the functioning of government entities. Also, the Law on Information Security (2016), in its article 6, sets out the list of Critical Information Infrastructure (CII) systems and networks which are known as **ICT systems of Special Importance**. It was said that the CII assets enlisted there were recently revised and updated through an amendment to the law which was passed late in 2019.[33]

93. The Law on Information Security defines ICT Systems of Special Importance as the systems used for specific activities, such as tasks in public sector bodies, activities of general interest (e.g. energy, transport, finance, health, information society services, etc.) and personal data processing (article 6). This law sets out a number of provisions which aim at the protection measures for ICT Systems of Special Importance (article 7), including the notification of cyber incidents to the Competent Authorities (article 11) and the establishment of international cooperation and early warning mechanisms (article 13).

94. As mentioned, the Law on Information Security was recently amended (2019) to (i) integrate some provisions of the Directive on Security of Networks and Information Systems (NIS Directive) and other EU laws, and (ii) to revise the list of the ICT Systems of Special Importance in the country. Those amendments will strengthen the current legal framework to ensure (a) the protection of the ICT Systems of Special Importance, and (b) strengthening of the capacity building in the national CERT, amongst others.

95. Focus groups also revealed that coordinating bodies, including MoI and MTTT, are presently drafting secondary regulations (bylaws) to provide further instructions (including the criteria for CI identification) on how to protect the critical infrastructure assets in Serbia adequately. During the CMM review, it was said that those bylaws will likely be adopted in the first quarter of 2020; however, the review team was recently informed that the bylaws which regulate CI are still under development and the bylaws which regulate CII were recently adopted.[34] Some government stakeholders pointed out that a new body will be created within MoI to coordinate and supervise the CI operators, but operators of ICT Systems of Special Importance will continue to be supervised by MTTT. Both MoI and MTTT should work closely to ensure that all sectors and actors within the whole CI and CII ecosystem are adequately protected in Serbia.

[33] https://www.ratel.rs/uploads/documents/empire_plugin/5e9f4832cdb97.pdf
[34] https://mtt.gov.rs/en/download/r2.pdf

96. It was noted that the financial sector institutions, with the support of the National Bank, have established robust security measures at the organisational level. Some participants pointed out that maintaining the highest security standards in the fast-changing cyber environment is a challenge for financial institutions. Overall, the environment in the financial sector looks very positive, both public and private institutions are totally committed to delivering both secure services and awareness-raising campaigns to their customers.

97. Some government participants pointed out that most of the cyber incidents in the telecom sector are directed at users, not at the operators. The vast majority of those incidents are successfully filtered and contained by the network operators. It was noted that there are between 10 and 20 network owners in Serbia, which have developed sufficient capacity to contain those cyber incidents. However, there are more than 200 small operators which probably do not have the same capacity. Therefore, those network owners are collaborating with small operators to enhance their level of security. It was noted that this issue had been already identified and actions were being taken. RATEL and all telecom operators understand the importance of taking adequate security measures to deliver secure services to their users.

98. Other public operators of ICT Systems of Special Importance pointed out that they follow both the IT security recommendations provided by the Office of IT and e-Government and other European agencies or associations and the applicable provisions of the Law on Information Security to ensure that their systems and networks are protected. They have internal IT security teams which monitor their ICT infrastructure and handle their incident response management process. In turn, these internal teams are supported by the Government CERT. It was noted that the customer service of this particular CERT has to be improved, mainly the incident reporting means.

99. It was shared that public operators of ICT Systems of Special Importance also have security policies and procedures in place, including sector-specific standards (e.g. NERC standards) and staff training policies -which have become a standard in the country. Some of those operators have their own recovery centres. They are either ISO 27001 certified or working towards that certification. Many of the security actions taken are not even prescribed by law, but the operators understand the relevance of cybersecurity for their operation, so they go one step ahead by acquiring (or working towards) these certifications.

100. Concerning incident reporting, the operators of ICT Systems of Special Importance are currently obliged to report immediately any cyber incident which has a significant impact on information security of the ICT systems, to the competent authority, that is MTTT (portal), or to the national CERT (portal). In the financial sector, the competent authority is the National Bank of Serbia, and RATEL is the competent authority for the telecom sector; therefore, the regulated organisations within those two sectors have to report their cyber incidents to those competent authorities, respectively. Then, both the National Bank and RATEL are obliged to report through the single system all the reported cyber incidents from their community members (financial institutions and telecom operators, respectively). Those incident reporting obligations are stated in article 11 of the Law on Information Security and article 2 of the Regulations on the incident notification procedure in information and communication systems of special

importance.[35] It was said that even though each body has independent channels for incident reporting, they are using the same reporting platform, so all information, including reported cyber incidents, is exchanged amongst them in real-time (Single system).

101. For those operators of the ICT Systems dealing with classified information will proceed per the regulations governing the field of classified information protection. The above incident reporting rule does not apply to the Independent ICT system operators due to the fact that they have their own CERT.

102. Within the National Bank, there is a specialised unit which has the capacity to assist all financial institutions in managing and mitigating the adverse impact of cyber incidents. Within RATEL, there is not a specialised unit, but telecommunications operators are directly assisted by the national CERT. It was also noted that the Association of Serbian Banks is working towards the establishment of a sectoral CERT to enhance the incident response capacity of the banks in Serbia. The Petroleum Industry of Serbia also has its own internal CERTs.

103. According to the Law on Critical Infrastructure, CI operators have to designate a liaison officer to serve as a focal point between the subject operator and MoI (article 9) to ensure the fulfilment of the obligations and tasks prescribed by law. It was said that the regulated organisations within both financial and telecommunications sectors had established efficient channels of communication with the pertinent regulator to share information regarding vulnerabilities, common risks and threats, and other cyber-related issues.

104. At the sectoral level, it was noted that regulated organisations in those sectors were sharing information amongst themselves. It was also noted that the financial sector was more advanced than any other sector regarding information sharing. For instance, the Association of Serbian Banks established six years ago an information safety board as a platform to exchange information and knowledge amongst its members. A web-based portal was created for its members to report cyber incidents and also to interact with other actors within the ecosystem, including law enforcement agencies and regional banking entities. In other sectors which also manage ICT Systems of Special Importance, information sharing varies considerably. For instance, in the energy sector information sharing is *ad hoc* or non-existent, according to some review stakeholders.

105. The Law on Critical Infrastructure obliges CI operators to implement, amongst others, a ***Risk Management Operator Security Plan*** (including *annual Risk Assessments*), the implementation of which is supervised by MoI (article 8). The review participants shared that within the financial sector, most of the regulated institutions conduct comprehensive risk assessments annually, which cover cybersecurity components, and they are audited by the National Bank. Some participants pointed out that telecommunications operators regularly conduct risks assessment at the organisational level, with cybersecurity being one of the assessed components.

106. It was noted that telecommunications operators are not supervised by RATEL from the cybersecurity perspective; however, MTTT conducts some supervision to all operators of ICT systems of Special Importance, including telecommunication

35 https://mtt.gov.rs/en/download/1(2)/Law%20on%20Information%20Securty%20(Sl.%20glasnik%20RS%206-16,%2094-17%20and%2077-19)(2).pdf and https://mtt.gov.rs/en/download/r2.pdf

operators, according to the applicable legislation. It was unclear if MTTT monitors the implementation of risks assessments or other security measures within the telecom. In other critical sectors, the implementation of risk assessment activities varies considerably. It was noted that penetration testing activities are conducted by most of the critical operators.

107. Some participants pointed out that no cyber drills have been organised within the financial and telecom sectors and other critical sectors; however, in 2017 there was one cyber drill organised by OSCE for the energy sector.[36] It was also recognised by the stakeholders that regular cyber exercises should be organised at the sectoral level or at least ensure that critical operators participate in any national-level cyber drills. Some participants pointed out that some operators of ICT Systems of Special Importance have participated in previous Tesla Cyber Drills.

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: Formative

108. EU laws and directives emphasise that establishing crisis management and communication procedures are highly important in case of a major cyber incident *which could jeopardise the stability and national security of the member nations. Various government agencies and ministries of Serbia, a candidate country to the EU, have taken multiple actions relating to crisis management, but not in a nationally coordinated matter.*

109. Despite the above, it was noted that MoI had established robust policies, strategies and laws and a coordination body regarding national disaster management (sector for emergency management).

110. It was also noted that cybersecurity activities were recently integrated into the crisis management structure of Serbia. For instance:

> a-) article 11 paragraph 14 of the Law on Information Security prescribes "… [i]n the event of threats, disturbances of destruction of an ICT system of special importance, the management and coordination of the implementation of measures and tasks in the said event shall be undertaken by the national emergency management office, in accordance with the law."
>
> b-) article 8 of the (new) Regulation on Incident Notification Procedure in Information and Communications Systems of Special Importance prescribes *"… [i]n case of an incident which is assigned the threat level of "Very High" in*

[36] https://www.osce.org/secretariat/351176

compliance with the Classification, the National CERT shall without delay notify the Ministry thereof, which shall then notify the Republic Emergency Management Authority that shall act in compliance with the competencies laid down by the regulations." As noted, these two provisions apply to the CII operators only; therefore, they do not have a national reach.

111. In addition to the enactment of those legal provisions, Serbia has taken the following actions in the cyber crisis management arena:

- MoD has organised, for the fourth time, a cyber drill called "Cyber Tesla"; however, this cyber simulation is not yet considered a national-level exercise. It was noted that not all relevant actors are part of it and some of them participate as observers, such as some private sector organisations. Its scope and community have to be expanded if the intention is to use this platform as a national-level exercise. It was noted that in the 2019 edition of the Cyber Tesla, private sector organisations had an active participation.

- MoD, and its internal bodies, is enhancing its cyber-defence capacity, which is certainly aligned with the crisis management capacity of the nation.

- During the CMM review, it was unclear whether the national CERT would take the lead to organise regular cyber drills at the national level. There are other bodies, such as the Body for Coordination and the National Security Council, which can take the lead or collaborate with the crisis management matters. After the CMM assessment, the review team was informed that the national CERT plans to organise the first national cyber drill in 2021 which is an important step to enhance the crisis management component.

- It was noted that the national CERT, with the cooperation of Microsoft, has developed a virtual platform for simulation of cyberattack. This scalable system aims to conduct technical trainings and cyber drills (blue vs. red) and is an efficient solution designed to enhance the knowledge and skills of the national CERT's staff members to detect cyberattacks and respond to them in a timely manner. During 2019, this system was used to train CII operators and also to conduct one cyber drill for Independent ICT system operators.

- It was also noted that some public servants and military officers had been trained in crisis management matters, both locally and internationally, by international organisations, such as NATO, CMU, OSCE. Indeed, there is some level of expertise in different public and private organisations.

- In 2017, Petnica Group, in collaboration with OSCE and other stakeholders, organised the first national policy-focused cyber drill in Serbia. Through simulating the practical application of the existing policy and legal framework, this cyber drill analysed the efficiency of existing procedures for crisis management, as well as the readiness of key public and private actors to apply these, highlighting good practice but also existing and potential challenges and obstacles in crisis communication. The final report of this exercise detailed a series of key conclusions and recommendations and also contained an overview of key challenges and obstacles arising from the existing legal framework and realistic capacities of the actors involved.[37] Indeed, this cyber

[37] https://www.osce.org/mission-to-serbia/404255?download=true

drill assessed several relevant aspects and its recommendations which could be taken as feedback to build a robust cyber crisis management structure in Serbia.

112. With the guidance of ENISA, MTTT and the national CERT, MoI (or its emergency management body) should consider taking the following actions: 1) to designate a national coordination body for cyber crisis management issues which has to be well-equipped to deal with cyber scenarios at the national level (if already in place, its legal mandate has to be broaden), 2) to define clear roles and responsibilities amongst the relevant stakeholders, and 3) to establish cyber drill planning and deployment procedures, including identification of relevant stakeholders, an adequate budget line, robust training policies, and monitoring and evaluation mechanisms, amongst others.

D 1.5 CYBER DEFENCE

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.

Stage: Formative to Established

113. The Ministry of Defence (MoD) is the government body responsible for protecting the Republic of Serbia from military and non-military challenges, risks and threats which can jeopardise the security of the country, its people, material resources and environment.

114. Within the defence structure, there are multiples agencies which are part of the cyber-defence operations and activities, including but not limited to:

- ***the Serbian Armed Forces*** (SAF) which are responsible for defending the country from external armed threats, and executing other missions and tasks per the Constitution, law, and the principles of international law regulating the use of force.[38]
- ***the Military Security Agency*** (MSA) is responsible for security and counterintelligence protection of the MoD and the SAF. As a part of this function, MSA carries out general security, counterintelligence and other activities and tasks of importance for the defence of the country.[39]
- ***the Military Intelligence Agency*** (MIA) is responsible for conducting intelligence activities of importance for defence on the collection, analysis,

[38] http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/zakoni/Law%20on%20Defense.pdf

[39] http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/zakoni/Law%20on%20Military%20Security%20Agency%20and%20Military%20Intelligence%20Agency.pdf

assessment, protection and transfer of data and information on potential and real threats, activities, plans or intentions of foreign countries and their armed forces, international organisations, groups and individuals.[40]

- ***the MoD CERT***. According to article 19 of the Law on Information Security, MoD CERT is one of the four government-related CERTs in Serbia that operate under a special regimen. It was noted that the MoD CERT is in charge of protecting the military ICT infrastructure from cyber threats. The staff of the MoD CERT is regularly trained locally and internationally. Human, technological and financial resources are adequate to fulfil the assigned mission. Retaining skilled officers and developing specialised skills are two of their main challenges. In addition to its core function, MoD CERT carries out awareness-raising campaigns, helps to develop security policies and procedures, amongst others.

115. The Government recognised in the SDIS that "… [i]nformation security is a key part of a comprehensive national security based on the information security of institutions, forces, people, systems, processes, information and values that are important for the security and [defence] of the country. The information and communication infrastructure, and the [defence] system services and data have a special significance for the national security of the Republic of Serbia." It denotes that Serbia has a good level of awareness that the cyber-defence capabilities of the country have to be strengthened.

116. In view of the above, SDIS sets out the following actions:

- Establishment of clear roles and responsibilities within the national security and defence structures.
- Development of scientific, technological and industrial capacities necessary for the protection of information security in the country.
- MoD and the SAF will develop comprehensive capabilities for defence in the cyberspace, in accordance with the constitutional and legal competencies, missions and functions.
- The Serbian Security Services will develop comprehensive capabilities to protect the information security of Serbia, including the ICT systems of special importance (CII).

117. Serbia has not adopted a cyber defence strategy. During the CMM review, some government stakeholders pointed out that the Government was drafting a new National Security Strategy and a new National Defence Strategy. Following those actions provided by the SDIS, review participants considered that it was likely that those two strategies integrate cyber-defence operations and activities.

118. The CMM review team was recently informed that both strategies were adopted late in 2019 (right after the CMM assessment). After going through the content of both strategies, the CMM review team found the following cyber-related components in both strategies:

[40] http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/zakoni/Law%20on%20Military%20Security%20Agency%20and%20Military%20Intelligence%20Agency.pdf

a-) ***National Defence Strategy 2019***:[41] This policy recognises that (i) cyber-attacks on critical infrastructure facilities, cybercrime, and the spread of fake news and misinformation within the concept of hybrid and information warfare, amongst others, are real threats to the regional security and could adversely affect the well-functioning of the elements of the defence system. It is therefore necessary to continuously develop the technological and information protection of the defence system elements at all levels of the defence structures; and (ii) to protect the security of Serbia and its citizens, the cybersecurity capacities have to be improved. In this regard, a clear and coherent policy will be formulated, a network of competent entities to combat cyber-attacks and crime will be established in order to increase the resistance of information and communication systems to incidents, and cooperation between the public and private sectors in the area of cyber security will be improved. *It was noted that in terms of implementation of this national defence policy, an action plan will be developed so it is likely that this plan contains specific cybersecurity-related components and activities within the defence structures.*

b-) ***National Security Strategy 2019:***[42] This policy also recognises that (i) cyber-attacks, such as cyber espionage, attacks against CI, unauthorised breaches into classified information data bases and spreading false news and disinformation via social networks, are considered as challenges, risks and threats to the national security of Serbia; and (ii) the national security structure will continue enhancing capabilities and capacities for processing, transfer and protection of information and information-communication systems and defence against techniques of hybrid and information warfare in information and cyber space. Considerable attention is going to be paid to further development of the overall security culture of all citizens aimed at raising awareness on the required increase of security of an individual and society. *It was noted that in terms of implementation of this national security policy, an action plan will be developed so it is likely that this plan contains specific cybersecurity-related components and activities within the national security structures.*

119. MoD, with the support of its internal agencies, is in charge of the cyber-defence matters in Serbia. There is no Cyber Command and Control Centre established in Serbia.

120. It was noted that specific threats to national security, including cyber threats, have been identified. Cyber threats have been in the radar of the MoD for more than a decade. Some government stakeholders pointed out that it is likely that those strategies address this particular issue, including the protection of critical infrastructures and ICT Systems of Special Importance from cyber threats. What has to be clear to the rest of the community is what will be the role and specific functions

41 http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/2019/Strategy%20of%20Defence%20of%20the%20Republic%20of%20Serbia.pdf

42 http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/2019/Strategy%20of%20National%20Security%20od%20the%20Republic%20of%20Serbia.pdf

of MoD and its internal agencies with respect to the protection of non-military CNI assets from major cyber incidents.

121. Some participants pointed out that the current policies and legal framework, the SDIS and those two strategies would set clear roles and responsibilities for the national security and defence bodies which are dealing with cyber-defence matters.

122. It was noted that national security and defence bodies had established lines of communications to exchange information regarding cybersecurity matters. This good practice has been expanded to other government agencies, such as law enforcement agencies.

123. Since 2016, MoD, in collaboration with the National Guard of Ohio, has organised annual military cyber exercises ("Cyber Tesla"). The 2019 cyber drill focused on the defence of telecommunications and IT systems against cyber threats. Its primary goals were to build military capabilities of the defence structures and national CERT to defend the military ICT infrastructures from cyber-attacks and strengthen the cooperation links with relevant state-members, government agencies and private sector organisations.[43]It was noted that private sector organisations had an active participation in this cyber event.

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: Formative

124. Through the CMM review sessions, it was said that digital redundancy is a solved issue in Serbia. Internet network operators have been investing resources and implementing measures to enhance the communication redundancy capacity in the country.

125. It was noted that internet redundancy measures at the organisational level have been adopted in most of the private and public sector organisations, such as financial institutions and other CI operators. For instance, in Belgrade, service providers have established between five and seven data centres. It was also noted that mechanisms and procedures to have resilient, redundant and backup communication networks are set out within their disaster recovery and business continuity plans. It was also noted that in 2019 it was built a massive data centre for government and commercial use so this data centre currently enables better redundancy capacity and additional disaster

[43]http://www.mod.gov.rs/eng/14702/multinacionalna-vezba-cyber-tesla-2019-14702

recovery systems for government and commercial users. However, there are no coordinated and systematic actions at the national level.

126. The Serbian government, mainly its crisis management agencies, first responders and ISPs, have not convened to assess and identify the main gaps and overlaps in terms of emergency response assets, communications, and the roles and responsibilities of the authorities to maintain communications stable during a national-level crisis. Indeed, setting up the communication channels and backups (digital and non-digital) and determining which authorities are in charge of managing and coordinating this type of matters is highly important in case of a national crisis, regardless of its nature - cyber or non-cyber incidents.

127. It was noted that the cyber drill organised by Petnica Group in 2017 had identified a series of communication issues and gaps which may help to initiate the assessment process mentioned in the above paragraph. As noted, Serbia has implemented some actions in different fields, but it needs better coordination amongst the different stakeholders and integration of the existing initiatives to avoid duplication of efforts and misuse of resources.

RECOMMENDATIONS

128. 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 Serbia. 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 MTTT, as lead ministry, should consider the following actions to enhance the implementation process of the current SDIS:

i. Collect and record relevant metrics and statistics on the SDIS' implementation process. Also, these metrics and monitoring mechanisms should be reviewed to ensure that they are robust and properly tied to the overall activities, goals and objectives of the SDIS.

ii. *Monitor and evaluate the existing individual projects and initiatives stated in the existing Action Plan.*

iii. *Review the current roles and responsibilities of the relevant stakeholders, including identification of gaps and duplication of functions.*

iv. *Gauge implementing partners' performance and managing and implementing capabilities.*

v. *Revise budget allocation to ensure sufficient funds for the implementation of the SDIS projects and initiatives.*

R1.2 The above recommendations aim also at enhancing the planning, implementation, and decision-making processes for the new strategy which should be discussed during 2020.

R1.3 If the plan is to develop and implement a new national cybersecurity strategy, MTTT and the other coordinating agencies should consider taking the following actions:

i. *Conduct a national cyber risk assessment to revise and update the new strategy and its action plan to ensure that its content not only addresses the next-level components, including the continuity of the relevant unfinished projects but also reflects the current national priorities and demands to respond to the fast-paced environment (e.g. cybersecurity education and crisis management, still pending issues).*

ii. *Provide enough resources and strengthen the capacity of MTTT to lead the process of designing, developing and implementing the new strategy.*

iii. *Encourage the participation of key stakeholders not only in the SDIS review process and consultation process for the new strategy, but also in the promotion, implementation and review process of the strategic objective and projects of the new strategy.*

iv. *Promote public and private partnerships (e.g. Petnica Group), so that private sector organisations, civil society and other non-governmental groups could contribute with and assume a more leading role in the implementation stage of the new strategy.*

v. *Ensure that relevant metrics and monitoring processes and data are collected from the beginning and evaluated to inform decision-making and resources allocation.*

vi. *Establish a review mechanism and procedure in the new strategy to conduct (yearly or bi-yearly) evaluations of the new strategy's projects and activities to maximise investment, gauge priorities, and ensure an efficient implementation process.*

vii. *Ensure that the new strategy is aligned with other national priorities, strategies and plans to avoid duplication of efforts and misuse of resources.*

viii. *Ensure that a reasonable budget is allocated to finance the development and implementation process of the new strategy and other national cybersecurity issues.*

ix. *Consider implementing international standards and best practices in developing a national cybersecurity strategy. See the international standards and best practices set out in the "Guide to Developing a National Cybersecurity Strategy" developed by ITU, World Bank and other international organisations.*[44]

[44] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

R1.4 Ensure that the coordinating bodies (e.g. MTTT, MoI, National CERT), which are part of the governance structure of the National Cybersecurity Programme, have clear roles and responsibilities and that the whole ecosystem, including the general public, understands their roles and functions and how cyber incidents, risks and issues get escalated to higher levels of government.

R1.5 Strengthen the National Cybersecurity Programme not only to lead, provide direction and monitor the process of implementation of the SDIS/new cybersecurity strategy but also to coordinate other relevant cybersecurity activities at the national level.

INCIDENT RESPONSE

R1.6 The national CERT's scope, legal mandate, resourcing, operating procedures and performance should be reviewed to ensure that it operates as a national incident response body and be totally clear, especially on how the national CERT interrelates with the other local incident response bodies (described above).

R1.7 Ensure that the national CERT has clear processes and defined roles and responsibilities. The national CERT should consider reviewing or enhancing the following aspects:

i. *Review the internal procedures, policies and manuals to efficiently perform the functions, roles and responsibilities of the national CERT.*

ii. *Conduct regular cyber-related exercises designed to test the human, coordination and financial capacity.*

iii. *Strengthen the internal training policy to set out guidelines for regular training and collect metrics to assess the results of the national CERT's staff training.*

iv. *Establish mechanisms and tools to collect metrics and statistics to monitor and evaluate the effectiveness of the national CERT.*

v. *Consider expanding the technical capacities to handle sophisticated intelligence threat analysis/support in domestic and international environments and digital forensic investigations. Ensure that the pertinent legal mandate is granted to incorporate those new functions within the national CERT's scope.*

vi. *Provide sufficient resources (human, technological and financial) to continue delivering the awareness-raising programmes. Review the programme material regularly.*

R1.8 Ensure that the existing incident reporting framework also obliges private organisations (non-CII operators) to report, in a timely manner, cyber incidents to the national CERT.

R1.9 Use the existing platforms and develop policies and procedures to formally exchange information on cyber incidents and preventive measures amongst the key stakeholders at the sectoral, multi-sectoral or national level.

R1.10 Strengthen the communication channels between the national CERT and public and private sector organisations (including all CERTs described above) to timely react and respond to in a coordinated matter in times of crisis.

R1.11 Foster and enhance arrangements and mechanisms for regional and international cooperation to resolve incidents as they occur.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.12 Disseminate the list of CI and CII sectors and assets with identified risk-based priorities. Regularly re-appraise both CI and CII ecosystems following international standards to capture changes in the threat environment.

R1.13 Ensure that the public and private CIP/CIIP operators are implementing robust incident prevention, detection and response protocols, policies and standards.

R1.14 Ensure that the relevant regulatory bodies have the human, technological and financial capacity to monitor and enforce the existing CIIP legal framework, reporting requirements and any other regulatory framework to ensure that CII operators are adequately protecting the national CII assets.

R1.15 Ensure that MoI has the human, technological and financial capacity to monitor and enforce the existing CIP legal framework, and reporting requirements and any other regulatory framework to ensure that CI operators are adequately protecting the national CI assets.

R1.16 Ensure that the relevant regulatory bodies take actions to foster and strengthen the mechanisms for regular vulnerability disclosure with defined scope for reporting incidents between CI/CII asset operators and the government/relevant regulatory bodies. Also, ensure that the CI/CII assets are audited on a regular basis and that the audit outcomes are disseminated to relevant stakeholders.

R1.17 CI/CII owners and operators should also consider the following actions:

i. *Implementing and auditing international standards and best practices in security measures, guidelines control and protocols for CI/CII cybersecurity.*

ii. *Implementing regular audit practices to assess network and system dependencies, interdependencies, and vulnerabilities to inform*

continuous reassessment of CI/CII risk portfolio, technologies, policies and processes.

iii. *Implementing and monitoring cyber risk management assessment and processes supported by adequate technical security solutions, communications links and harm mitigation measures.*

iv. *Fostering and strengthening formal coordination and information-sharing mechanisms between CI/CII actors in both the public and private sectors.*

v. *Establishing formal coordination and information-sharing actions with other relevant actors of the CI/CII ecosystem. Moreover, building and fostering trust between government and CI operators concerning cybersecurity matters and exchange of threat information.*

vi. *Investing in capacity building for Board Members and Senior Leaders of CI/CII organisations, in both private and public operators, to understand cyber-risk intelligence so that they can lead in the face of crisis and take their part in risk management more generally.*

vii. *Allocating sufficient resources in proportion to the assessed impact of an incident to ensure a rapid and effective incident response.*

CRISIS MANAGEMENT

R1.18 Consider equipping the Sector for Emergency Management with a legal mandate and sufficient technological, financial and human resources to manage and coordinate with relevant actors (e.g. MTTT, national CERT) the cyber crisis management issues at the national level. Also, integrate the cybersecurity component into the national crisis management system, policies and structures.

R1.19 Ensure that the national CERT is equipped to support the Sector for Emergency Management during any cyber crisis at the national level.

R1.20 Consider implementing the relevant recommendations on cyber crisis management stated in the final report of the national policy-focused cyber drill (Petnica Group).

R1.21 Consider developing and implementing a national cybersecurity incident response plan (or similar arrangement) which identifies relevant actors, establishes clearly their roles and responsibilities in case of a crisis and outlines the procedures to manage the kind of scenarios resulting from major cyber incidents to promptly respond to and recovery from that type of incidents.

R1.22 This incident response plan should contain planning procedures for regular national cyber exercises, addressing the following aspects:

i. *Ensuring that such a planning process includes engagement of participants, outlining roles in the exercises, and the articulation of benefits and incentives for participation.*

ii. *Prioritising cyber crisis management exercises, especially at the public and private sectors, CI/CII community and national level, and communicate the value of these exercises to all sectors and relevant actors (e.g. national CERT) of the ecosystem. To allocate the appropriate resources to conduct such exercises.*

iii. *Identifying metrics, including the feedback provided by the participants and stakeholders, to evaluate the success of the exercise. Evaluate the exercises and feed the findings back into the decision-making process.*

iv. *Conducting compromised communications scenarios and exercises to test emergency response asset interoperability and effective functionality and incorporate the results of the exercises to inform strategic investment in future emergency response assets.*

v. *Sharing evaluation of the crisis management exercises with the international community so that lessons learned can contribute toward an improved global understanding of crisis management.*

CYBER DEFENCE

R1.23 Strengthen the cybersecurity capacity within the MoD (which includes its internal bodies), including allocation of sufficient human, financial and technological resources, to adequately monitor and protect the military ICT infrastructure from adverse cyber incidents.

R1.24 Ensure that the actions plan of the National Defence and National Security Strategies (described above) clearly define the scope, roles and responsibilities of the defence and national security actors within the cyber defence arena as per the broader cybersecurity needs of the country.

R1.25 Foster international cooperation mechanisms to exchange cyber intelligence information with allies and other regional platforms.

R1.26 The communication channels and collaboration mechanisms amongst the national CERT, the MoD CERT and the CERT of the Intelligence Service Agency should be strengthened.

R1.27 Expand coordination in response to malicious cyber-attacks on police/military information systems and critical infrastructure assets (following the instructions

provided by the National Security Strategy 2019 and the National Defence Strategy 2019).

R1.28 Establish robust training programmes for CERTs, armed forces, and national security's staff members working on cyber defence issues in the country and develop awareness campaigns.

COMMUNICATIONS REDUNDANCY

R1.29 Establish a consultation process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response assets communications and authority links, and also identify and map emergency response assets, priorities and standard operating procedures in case of communication disruption.

R1.30 Allocate appropriate resources not only to activities, such as hardware integration, technology stress testing, personnel training and crisis simulation drills but also to ensure that the redundancy efforts are communicated to relevant stakeholders.

R1.31 Consider implementing the relevant recommendations on communication redundancy stated in the final report of the national policy-focused cyber drill (Petnica Group).

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

129. Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet 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.

130. 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: Formative

131. Awareness of cybersecurity issues in Serbia is substantial and growing, but with key actors in all sectors, and the general public, displaying various degrees of knowledge regarding cybersecurity risks. In the government, many participants indicated that the awareness of cybersecurity risks and the adoption of good practices by staff members

in key departments was growing, mainly due to recurrent cybersecurity awareness training. Participants also noted that the Law on Information Security required some ministries, as custodians of systems of special importance, to establish policies and good practices, and awareness workshops have been normally a component of these policies. Participants also credited the communication activities of the National CERT for an increase in awareness. Most participants agreed that, within the government, staff members would not, for example, simply place into their computer a memory stick they found lying around but would instead hand it to their local authorities to handle. However, awareness training for government employees is not currently mandatory and is not applied uniformly across the government ministries. There is also no on-boarding of cybersecurity awareness for new employees in the government or a briefing on the policies and practices that apply.

132. A further concern that emerged during discussions was related to local governments. While there are efforts to enhance the cybersecurity capacity of government staff and officials at the national level, more needed to be done to bring the local governments up to a comparable level.

133. In the private sector the mindset depends on the particular industry and size of a company. Within the larger companies, particularly those with more international presence, and most if not all the financial services and technology companies, the cybersecurity mindset is high. Participants agreed that these institutions generally provided their staff with cybersecurity awareness training. However, amongst other companies, participants felt that there is a substantial variation and there was a suggestion that most of the small and medium-sized businesses did not consider cybersecurity risks until there was an incident that directly affected them. Other participants from organizations that provide technology services to private sector entities noted that there were indications that cybersecurity awareness in that sector was increasing, based on the requests for services offered and a perceived decrease in cyber-related incidents that required remediation.

134. Among the general public, the picture was less clear, as some participants noted that in certain cases the level of awareness has remained limited, while others presented a brighter picture. It was pointed out, for example, that the cybercrime services within the criminal justice mechanisms had seen a steady increase in the reporting of cybercrime, which was credited to an increase in the number of awareness training events being conducted by a range of public and private sector entities. It was noted that the criminal justice mechanisms, such as the public prosecutor's office, has conducted public awareness-raising activities and conducted media campaigns to raise awareness. It was also noted that the education system includes awareness-raising activities for students in primary and secondary schools. Nevertheless, there is a persistent belief among many participants that the general public, and young people, in particular, are not fully aware of the risks and do not regularly practice safe computing.

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: Formative to Established

135. As with awareness, trust in the Internet is substantial, but not always based on a full understanding of the risks. As noted above in section 2.1, cybersecurity awareness amongst the general public is increasing, but participants were not convinced that most users can recognize risks, such as potential phishing attempts or insecure web sites. There is a sense that most users accept what they see and do not always critically assess what they see or receive online.

136. Internet service providers offer basic security services, such as secure web services for hosting, but consumer-based services do not offer demonstrably secure services or information for their customers.

137. E-government services have been well developed in Serbia, and with the creation of the Office of IT and e-Government within the Office of the Prime Minister, this trend is set to continue. Serbia ranks 49th of all countries in the 2018 UN E-Government Survey, and 7th of 14 southern European countries. Through a government portal[45], a substantial variety of services are offered, including under the headings of, *inter alia*, family, health, education, finance and employment. These web-based services are all protected with secure connections, with the use of PKI certificates, and although relatively new, the Serbian Law on Personal Data Protection offers some measure of reassurance that the data collected and stored by these services are secure. While it is unlikely that the general public is well aware of provisions in the law, participants largely noted that these services are well-used and trusted by the general public.

138. E-commerce services are fully established by multiple stakeholders. In its 2018 B2C E-Commerce Index report, UNCTAD ranks Serbia as 41st globally in its e-commerce index, and second of ten "transition economy" countries, demonstrating the growth of the nation's public e-commerce environment. Participants largely supported this assessment, noting a robust use of local e-commerce offerings, as well as purchases from global companies, such as Amazon. Participants also noted that online and mobile banking is trusted and frequently used, and online payment systems are well-established.

[45] https://www.euprava.gov.rs/?alphabet=cyr

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: Formative

139. In 2018 Serbia adopted a Law on Personal Data Protection. Applicable from mid-2019, it has been generally modelled after the EU's General Data Protection Regulation (GDPR). As this law is very new, many review participants found it difficult to assess its likely impact on the data protection environment in Serbia. They noted that it is a complex piece of legislation, and at the stage of assessment it was difficult to predict the impact it would eventually have. It was noted that implementation of data protections in the country remains at a very low level, with considerable confusion regarding the requirements for compliance with new regulations.

140. It was generally agreed by participants that Serbian society was at the early stages of awareness regarding the need to protect personal information. It was noted that many individuals freely enter personal information in order to access free online services. It was also mentioned that only a small number of social media users in Serbia were fully aware of the risks of posting personal information online, and most were not very familiar with the privacy settings that these services offered.

D 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: Established

141. According to participants from both the public and private sectors, there are established mechanisms for reporting various types of cyber incidents, the most visible of these is the "Report an Incident" button on the home page of the national CERT[46] and MTTT[47]. This mechanism allows for the filing of reports on any one of more than 20 types of incidents, including data breaches, viruses, phishing, identity theft and cyberbullying. This reporting mechanism was well-known by all stakeholders throughout the assessment, an indication of the success of the marketing of this mechanism.

[46]https://www.cert.rs

[47]https://mtt.gov.rs/prijava-incidenata-u-oib/?script=cir

142. Review participants also noted that there is a department for cybercrime within the police department, but a common channel for reporting incidents of cybercrime is the web page of the special prosecutor's office for hi-tech crimes. This mechanism is well established, although it was suggested that it could be improved through the implementation of a hotline for more direct reporting. In addition, participants noted the existence of the National Contact Centre for Online Safety of Children[48], a portal dedicated to providing advice and reporting harmful and disturbing content on the Internet. Reporting through the use of this mechanism is also available through a special telephone number which not only allows for the reporting of an incident, but also contains material useful to parents and children on the ways to cope with such incidents. These mechanisms are presented to children in schools and there are also sessions with parents to inform them of the channels for reporting and the materials available to support them.

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: Formative

143. In Serbia there appears to be some media coverage of cybersecurity topics, but only in an *ad hoc* manner. A review of the popular news web sites confirms this observation, as very few stories related to cybersecurity or cybercrime were apparent. Participants, however, noted that the local press had covered some international cybersecurity-related events, such as the stories around the hacking of the US elections, as well as local specialized events, such as awareness workshops conducted by the national CERT or other organisations. However, the National CERT has worked to improve the awareness of local press to the issues surrounding cybersecurity. Specifically, it was noted that the national CERT organized a workshop for representatives of media outlets. During this event, titled "Active and Safe on the Internet" the national CERT presented its role and responsibilities, and explained the provisions of the Law on Information Security and Information Security Act as well as conducting a cyber drill for members of the press. The local media reported on this activity[49] [50]. As a follow-up activity to the workshop, the national CERT created a network of media reporters interested in cybersecurity. This media cohort is used as one channel for the recommendations and notifications from the national CERT to the

[48] www.pametnoibezbedno.gov.rs

[49] http://www.rtv.rs/sr_lat/drustvo/kako-da-budete-bezbedni-na-internetu!_1052688.html

[50] http://www.personalmag.rs/ratel-radionica-simulacija-hakerskog-napada-povodom-obelezavanja-medunarodnog-meseca-informacione-bezbednosti/

public. In addition, RATEL, the telecommunications regulator, regularly distributes press releases regarding cybersecurity activities[51]

144. Participants also noted that they were aware of only limited discussions on social media regarding cybersecurity. The telecommunications regulator, RATEL, which is the home of the national CERT maintains links to social media sites, including pages on Facebook, YouTube and LinkedIn.

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *cyberculture 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 Ensure that all government employees, including senior officials, receive regular cybersecurity awareness training. Consider centralizing the administration of the training and consider establishing the training as a regular component of on-boarding new employees.

R2.2 Establish a programme to bring cybersecurity awareness training to government employees and officials at the local level.

R2.3 Create or enhance cybersecurity outreach programmes targeting small and medium-size businesses to raise awareness of the importance of securing their systems. Building relationships with service providers may offer a channel to reach these business entities.

R2.4 Working with the appropriate education authorities, create and implement a method of evaluating the cybersecurity awareness level of the nation's youth.

TRUST AND CONFIDENCE ON THE INTERNET

R2.5 Encourage ISPs to create easily accessible materials (i.e. prominently displayed on their home pages and distributed through their social media accounts) that promote good cybersecurity practices and trust in their services.

[51] https://www.cert.rs/en/vesti-arhiva-2018.html; https://www.cert.rs/en/vesti-arhiva-2019.html

R2.6 Ensure the monitoring of the use of e-government services and respond with declines in usage with media campaigns that highlight the effectiveness and security of these services.

R2.7 Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.8 Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online. Secondary and tertiary educational institutions may wish to develop and deploy special modules dedicated to practical aspects of personal data protection.

R2.9 Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

REPORTING MECHANISMS

R2.10 Continue to develop and deliver awareness programmes that promote the regular use of reporting mechanisms by the general public.

R2.11 Develop programmes for the private sector that highlight the use of reporting mechanisms as an investment in loss prevention and risk control.

MEDIA AND SOCIAL MEDIA

R2.12 Encourage media to more fully focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts, especially as they pertain to Serbian society (i.e. endeavour to focus on local content).

R2.13 Develop programmes and campaigns to raise awareness among media providers and leading social media actors, especially during the Cybersecurity Awareness Month (October).

R2.14 Use existing government social media channels to encourage a frequent discussion of cybersecurity issues.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

145. 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: Formative

146. Serbia has several mechanisms in place that support cybersecurity awareness-raising for a broad range of stakeholders. The national CERT has the primary responsibility for awareness of citizens, businesses, and public entities regarding the importance of information security, including risks and protection measures, and implements campaigns aimed at raising this awareness. For citizens it publishes recommendations, comments and brochures with cybersecurity protection information on its website. For the other target groups, it developed workshops, operational since 2019. The mandate for these activities by the national CERT is outlined in Article 15[52] of the Law on Information Security. It was noted that the website of the national CERT was created in September of 2018, and that the CERT staff have since monitored the website statistics. These statistics, coupled with consultations amongst the staff of the CERT, are used, to plan the content of future materials.

[52] Item 5 of the Article states that the national CERT shall: "raise awareness among citizens, business entities and public sector bodies about the importance of information security, the risks and protection measures, including the implementation of campaigns aimed at raising this awareness"

147. Recently, the national CERT has released a new campaign to coincide with the National Cybersecurity Awareness Month, called “active and safe on the Internet”. This was in the form of a video published on the RATEL YouTube page. The national CERT, through the RATEL social media outlets, also offers materials and messages focused on cybersecurity.

148. A different mechanism is offered by the MTTT which focuses on the protection of children on the Internet. Its National Contact Centre for Safety of Children organizes educational campaigns and raising awareness through television programmes and videos that raise awareness on the importance of protection of children on the Internet. This also includes a website[53], known as “smart and safe” which includes materials on protecting children on the Internet, including against threats and risks. The material on this website was developed by the Ministry in cooperation with stakeholders, including UNICEF, and other child development professionals.

149. In addition to these programmes, the Share Foundation[54], a Belgrade-based “nonprofit organization established in 2012 to advance human rights and freedoms online and promote positive values of an open and decentralized Web, as well as free access to information, knowledge, and technology” has in the past few years conducted more than 100 trainings with the topic of digital security with civil society organizations and the media. It also developed educational videos that cover, *inter alia*, digital safety and security, as well as issues of Internet and computer literacy. These were broadcast on four TV stations in Serbia and in Montenegro. The Foundation also offers video materials on these topics that are distributed through the Internet and TV stations. It was noted that although this was not the Foundation’s core function, it was filling a need that was, at the time, unaddressed.

150. Other initiatives were mentioned by participants, including special awareness trainings organized for specific communities, including skills enhancement for law enforcement and seminars directed towards the technical community.

151. Few or none of these initiatives keep detailed metrics on the results of the campaigns or trainings.

152. There are currently very few awareness programmes directed towards executives. According to participants, there have been occasional workshop for small and medium-sized enterprises, organized through the Serbian Chamber of Commerce, and these have been well-received. Participants indicated that, in general, executives from financial services and telecommunications companies have a better than average awareness of the risks of cybersecurity. There was no indication that executives of critical infrastructure operators received cybersecurity awareness training.

[53] www.pametnoibezbedno.gov.rs

[54] https://www.sharefoundation.info

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: Formative to Established

153. Serbia, through the SDIS and its Actions Plan and other national policies, has recognised the need to enhance the ICT and cybersecurity education in primary and secondary schools and universities; however, the SDIS Action Plan sets out few initiatives in this particular area.

154. At the school level, the Ministry of Education, Science and Technological Development (MEST) developed mandatory IT training courses, with basic cybersecurity components, for children in primary and secondary schools. Primary school materials are very basic in content, while secondary school materials are more sophisticated, with professors regularly engaged in material adaptation and revision. Those IT training courses are taught in both public and private schools.

155. At the university level, MEST (leading ministry) recently mapped some relevant tertiary education institutions and also recommended some special study programmes on information security in relevant universities. These two actions are expressly described in the SDIS Action Plan.

156. It was also noted that at least nine universities in Serbia offer accredited cybersecurity-related laboratories or courses within their degree programmes - undergraduate, graduate and post-graduate/doctoral. Some participants pointed out that the following courses are being offered in Serbia:

- University of Belgrade – School of Electrical Engineering: Computer Security course (Bachelor's degree)
- University of Belgrade – Faculty of Organizational Science: Computer System Security course (Undergraduate degree) and Security Techniques in Computer Networks course (Master's degree)
- University of Novi Sad – Faculty of Technical Sciences: E-business System Security course (Bachelor's degree) and Security and Safety in Electric Power Systems course (Master's degree)
- University of NIS – Faculty of Electronic Engineering: Information Security course (Bachelor's degree), Computer Network Security course (Master's degree), Cryptography course (Master's degree), Secure Software Design and Implementation course (Master's degree), Digital Forensics course (Master's degree)
- Subotica Tech – Computer Network Administration course which contains information security topics in the programme, and E-Commerce course which contains topics, such as cryptographic algorithms, the security of webs, etc.

- University of Kragujevac – Faculty of Technical Sciences: Data Protection course (technical), Networks Security and Protection course, and Protection of Computer Systems course.
- Academy of Criminalistics and Police Studies (KPA): Cryptology course (Bachelor's degree), Data and Information Security course (Bachelor's degree), Authentication Systems course (Bachelor's degree), Advanced Systems for Biometric Identification course (Master's degree), Digital Forensics course (Master's degree), Detection of Network Attacks course (Master's degree), Anti-hacking tool course (Master degree), High-Tech Criminal course (Master's degree), and Information System Management and Security course (Master's degree).
- The School of Computing: Software testing and security course, security and cryptography course (Bachelor's degree), cryptography and cryptanalysis (PhD's degree).
- Belgrade Metropolitan University (BMU): Operation Systems Security course (Master's degree), Security of Computer Networks course (Master's degree), Cryptography and Crypto Technology course (Master's degree), Safe Software Engineering course (Master's degree), Database Security course (Master's degree), Computer Forensics course (Master's degree), and Analysis of Advanced Algorithms course (Master's degree). It is important to mention that these BMU courses are all part of the Master's degree mentioned in the next paragraph.[55]

157. Except for a master's degree in cybersecurity given by BMU, it was noted that there are not any dedicated cybersecurity degree programmes in Serbia. The courses described above are part of the IT or computer science degree programmes. Some participants said that those courses are either mandatory or elective. Optional courses also have a high enrolment rate.

158. It was noted that in those universities mentioned above cybersecurity education is not always subsidised by the Government. In one university, the number of registered students is very low (27 students) due to the fact that all students are subsidised by the Government. In other universities, some students are either subsidised or self-financed. It was said that students who are subsidised are not obliged to work for the Government, except for those students who are in the military sector.

159. Even though the Government, through some of those universities, allocates financial resources every year to cover student subsidies, some government stakeholders stated that there is not yet a national dedicated budget for cybersecurity education. It was noted, however, that IT education does have a national dedicated budget.

160. It was shared that most of the courses described above are technical-oriented, but a couple of courses study the human aspects of cybersecurity. Review participants noted that only one university offers a PhD programme in cybersecurity and the rest of those courses described above range from undergraduate to master's degree programmes. Some stakeholders pointed out that in the last ten years only one university has graduated more than 3.000 IT experts with security skills.

[55] https://www.metropolitan.ac.rs/en/master-studies/information-security/

161. Some stakeholders from academia pointed out that most of the above universities have established roundtable discussions with the industry to review their curricula. Some universities consult with the industry every three or four years regarding any update to the curricula or new academic programmes to ensure meeting the industry needs. For instance, it was recently discussed in a working session that universities should develop more training programmes for data protection officers since there are not enough professionals in Serbia with the required education and skills.

162. Some participants pointed out that academics are highly qualified. Most of them hold PhD degrees and are constantly trained locally or internationally. At the moment, the number of academics is sufficient to deliver those courses described above. It was noted that those academics usually work either full-time (programme coordinators) or part-time (lecturers or visiting professors). It was unclear whether there are qualification programmes for cybersecurity educators in Serbia.

163. It was noted that no courses are addressing cyber policy issues in the country. Also, cybercrime or cybersecurity-related courses are not taught in local laws schools. However, there are two master's degree programmes, one specialised in national security and the other in cybersecurity and protection of personal data protection (new) which address cybersecurity matters from the legal perspective. It was noted that some of the lecturers in those programmes have a legal background.

164. It was said that cybersecurity education in Serbia, especially at the university level, requires a holistic approach for graduates to have a broader view of the cybersecurity issues, i.e. being able to understand relevant technical, legal and policy matters. It was noted that some actions have been taken to adopt this approach in tertiary education.

165. Some participants pointed out that a few universities occasionally offer short courses or seminars for non-specialists. For instance, cybersecurity courses have been given to customs and tax administration staff members.

166. It was noted that a few universities are presently conducting research and development projects in cybersecurity, but still have low impact. It was said that one university had recently built and equipped a modern laboratory to develop some cybersecurity research and development projects which are led by a small team of researchers.

167. Some participants recognised that there are sufficient cybersecurity professionals in the country. Some government stakeholders confirmed that there are no records within the employment authorities of any unemployed cybersecurity professional. Despite the above, it was noted in multiple sessions that, in general, the cybersecurity education capacity in Serbia needs to be strengthened, and the Government has to elaborate a comprehensive action plan.

168. Some stakeholders pointed out that the above universities are graduating enough IT security professionals to supply the needs of the domestic market. It was noted that experienced security experts emigrate to other countries looking for better salary conditions and professional opportunities.

169. It was also mentioned that there is a high fluctuation rate of personnel within the public sector because the salaries in the private sector are much higher. As a result, public sector organisations are having problems retaining skilled cybersecurity experts as those organisations are not allowed by law to hire new staff due to some budget restrictions.

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.

Stage: Formative to Established

170. Stakeholders from different sectors recognised the need to enhance the professional training capacity in cybersecurity, but it has not yet been documented at the national level. There is no specific project in that respect on the SDIS or its Action Plan.

171. It was noted that training programmes in cybersecurity are offered for public and private sector employees, as well as for the general public. However, training on cybersecurity issues for IT staff within public institutions is likely to be limited. Within the private sector organisations, cybersecurity training opportunities vary considerably.

172. ICT professional certifications with some security modules or components are available in Serbia.[56] For instance, CISCO and other private companies offer different levels of certification, such as Certified Network Associate-Security, Certified Network Professional-Security, Certified Internetwork Expert-Security.[57][58]

173. Internationally accredited IT Security and Governance training and certification courses are offered in Serbia. Experts can select from a range of courses, such as *IT Security and Governance Certification Courses, Foundation Level IT Security and Governance Certification Courses* (Ethical Hacking Foundation Training and Certification and COBIT 5 Foundation Certification Training Course), *Intermediate Level IT Security and Governance Certification Courses* (CGEIT Course) *or Advanced Level IT Security and Governance Certification Courses* (CRISC Course, COBIT 5 Assessor Certification Training Course, COBIT 5 Implementation Certification Training Course).

174. For those security professionals who want to learn or enhance their incident handling capacity, Trusted Introducer courses (including but not limited to Transit I and Transit II) are available for participants from Serbia.[59] For instance, national CERT's staff members are certified in those incident response courses.

175. Some stakeholders said that the demand for those industry certifications is increasing because public and private organisations require that individual security staff members hold this type of certifications. It was also noted that the high cost could be a constraint for both institutions and individuals to pursue these industry certifications.

[56] https://www.theknowledgeacademy.com/rs/courses/ccna-training/ccna-training-cisco-certified-network-associate/

[57] https://cpu.rs/education/cisco-sertifikati/

[58] https://www.viser.edu.rs/stranica/cisco-akademija?userLanguage=eng

[59] https://www.trusted-introducer.org/

176. Some stakeholders pointed out that the new Law on Data Protection, which is aligned with the GDPR and other EU directives, requires Data Protection Officers (DPOs) in every organisation to collect, store and process personal data. These professionals require some specialised training, so DPO certifications will soon become a requirement for them. Currently, there are a few DPO training options in Serbia.

177. It was noted that *adhoc* training courses, seminars, and online resources are available for cybersecurity professionals through public and private sources. For instance, the Serbian ISACA Chapter, which currently has 98 members, organises regular workshops,[60] meet-ups, and an annual conference in Belgrade.[61] It was noted that multiple cybersecurity conferences and seminars took place in 2019 in Serbia,[62] including the Belgrade Women's Cyber Forum 2019[63] and the QuBit Conference Belgrade 2019.[64] The Informatics Association of Serbia (IAS) also organises cybersecurity-related workshops for its members.

178. The Serbian ISACA Chapter, the Serbian Information Security Society, the eSecurity Association, and IAS also organise social and networking events, so that their members get together, interact and share knowledge in an informal environment. Petnica Group also leads a joint public and private effort in which information, knowledge and experience are exchanged amongst key stakeholders in the field. This particular group has contributed to the cybersecurity development in the country.

179. It was noted that knowledge transfer from employees trained in cybersecurity matters to untrained staff is practised occasionally, especially in the private sector. Within the public sector organisations, there is not a general policy in that respect, but a few government organisations have implemented this good practice.

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 Serbia. 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.

[60] http://www.isacaday.rs/en/#section-496
[61] https://engage.isaca.org/belgradechapter/home
[62] https://infosec-conferences.com/country/serbia/
[63] https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/CyberForum/Women%E2%80%99s-Cyber-Forum-2019.aspx
[64] https://belgrade.qubitconference.com/

AWARENESS RAISING

R3.1 Appoint, task and fund the national CERT (or another designated body) to engage relevant stakeholders from public and private sectors in the coordination, development and delivery of the awareness-raising programmes and materials.

R3.2 Task the designated body to develop a single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform.

R3.3 Task the designated body to develop evaluation measurements/metrics/statistics, based on the existing initiatives of the national CERT, to study the effectiveness of the awareness programmes to inform future campaigns taking into account gaps or failures.

R3.4 Task the designated body to consult with relevant stakeholders to develop and deliver dedicated awareness-raising programmes for executive managers within the public and private sectors, particularly focused on small and medium-sized businesses, as well as critical infrastructure operators.

FRAMEWORK FOR EDUCATION

R3.5 Coordinating bodies (e.g. MTTT, Ministry of Education) should define and inform cybersecurity education priorities through broad consultations across government, the private sector, academia, and civil society.

R3.6 Identified priorities should be integrated into the SDIS 2020 Action Plan (or into the revised action plan of the new strategy) accompanied by sufficient budget (aiming at the creation of a national dedicated budget) to accomplish the objectives.

R3.7 Create cybersecurity education programmes for academics and instructors to ensure that skilled staff is available in the country to teach newly-formed or existing cybersecurity courses.

R3.8 Integrate cybersecurity content in all (technical and non-technical) degrees at universities and develop specialised cybersecurity courses and degrees in universities and other higher education bodies to supply the domestic market's needs.

R3.9 Promote the multi-disciplinary nature of cybersecurity (its technical, legal, policy, business, among other aspects) in all tertiary courses.

R3.10 Expand the availability of cybersecurity and cybercrime courses to students of non-technical study programmes, such as law, national security, criminology or management studies.

R3.11 Promote efforts by universities and other academic bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists.

R3.12 Review regularly the material of the IT courses given by primary and secondary schools to strengthen its cybersecurity content. Develop and collect effective metrics to evaluate feedback from existing students and key stakeholders (including the industry) to ensure further development and enhancement of cybersecurity course offerings (tertiary education). Allocate additional financial resources for public universities to expand and enhance their existing infrastructure, including laboratories, equipment and other facilities, to meet the growing demand for formal education in cybersecurity.

R3.13 Develop public-private partnerships for sustainable and high-level research and development programmes at universities and other academic bodies. Also, allocate public financial resources for research and development programmes.

R3.14 Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, to enhance their expertise by combining education and practical training.

R3.15 Strengthen free-tuition programmes for university education and/or create a national fund for both scholarship and student loan programmes, so that students and professionals who want to initiate or strengthen their security career development can take cybersecurity degree programmes or professional certifications.

R3.16 Market Cybersecurity as an important career option by using different marketing methods. The Government and/or industry should consider creating competitions and initiatives for students to increase the attractiveness of cybersecurity careers.

R3.17 The Government, in collaboration with private sector organisations, should consider creating academic centres of excellence in cybersecurity.

R3.18 Consider creating and maintaining a defined incentive plan to keep experienced and skilled cybersecurity experts not only in the country but also in the public services.

R3.19 Consider appointing a designed body or committee, which in cooperation with all role players, should be responsible, among others, for coordinating the development of skills towards building a cadre of cybersecurity-specific professionals. As part of its functions, this body or committee should identify training needs and develop training courses and online resources for targeted demographics, including non-IT professionals.

R3.20 Develop a central portal for coordination and sharing training information for experts.

R3.21 Create and maintain a national-level register of cybersecurity experts.

R3.22 Ensure that affordable security professional certifications are offered across sectors within the country. Different forms of professional cybersecurity certification, e.g. ISACA certifications, will provide suitable skills at a faster rate. Consider subsidising the high cost of training and certification courses for trainees.

R3.23 Develop metrics to evaluate the take-up and success of cybersecurity training courses to strengthen the current offerings and inform future training programmes.

R3.24 Establish job creation initiatives for cybersecurity professionals and students within the organisations and encourage employers to create cybersecurity positions based on their needs and also train their staff to become cybersecurity professionals.

R3.25 Consider creating and implementing internal policies or special incentives to retain skilled cybersecurity professionals.

R3.26 Consider developing and implementing a formal knowledge transfer policy across all sectors to foster and promote this practice at all levels, government, private sector organisations, CI/CII operators, among other stakeholders.

R3.27 Promote the creation of networking platforms and/or professional associations which can organise cybersecurity-related events (seminars, workshops, etc.) and get cybersecurity professionals together regularly for training and networking purposes.

R3.28 Consider integrating into the SDIS 2020 Action Plan (or into the revised action plan of the new strategy) strategic objectives and activities to develop and strengthen the professional cybersecurity training capacities in the country.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

180. 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: Established

181. Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in Serbia.

182. In 2009, Serbia ratified both the Council of Europe (CoE) Convention on Cybercrime[65] and the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems[66].

183. The most relevant legislative frameworks related to Serbia's Internet and cybersecurity are:

- Law on Information Security (2016)

[65]Council of Europe (2001) Convention on Cybercrime, 23 November 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[66] Council of Europe (2006) Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

- Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (2017)
- Law on Electronic Government (2018)
- Law on Electronic Commerce (2009)
- Law on Personal Data Protection (2018)
- Law on Consumer Protection (2014)
- Law on Electronic Communications (2010)
- Law on Secrecy of Data (2009)
- Law on Copyright and Related Rights (2009)
- Regulation on the Safety and Protection of Children in the Use of ICT (2016)
- Criminal Code (2005)
- Criminal Procedures Code (2011)
- Law on the Organization and Jurisdiction of Government Authorities Fighting against High Technological Crimes (2005)
- Law on the Confirmation of the Convention on Cybercrime (2009)
- Law on the Confirmation of Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of racist and xenophobic nature committed through computer systems (2009)
- Law on the Confirmation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2010)
- Law on Military Security Agency and Military Intelligence Agency (2009)

*It was noted that all laws in Serbia, including those mentioned above, are publicly consulted as part of the drafting and enactment process.

184. Serbia has an all-encompassing legal framework that deals explicitly with cybersecurity. Its laws address cybersecurity-related issues, such as personal data protection, cybercrime offences, intellectual property protection of online services and products, child pornography, incident reporting obligations, protection of CII, security and integrity of electronic communication networks and services, handling of electronic documents in legal transactions, administrative matters, court and other procedures, amongst others.

185. The ***Law on Information Security*** created the basis for the establishment and implementation of a comprehensive information security framework. This law regulates protection measures against security risks in ICT Systems of Special Importance (CII), liability of operators of ICT Systems of Special Importance in the management and use of ICT systems, and also defines the competent authorities for the implementation of protection measures, coordination between security actors and monitoring of proper application of the prescribed protection measures.[67]

186. The Constitution of the Republic of Serbia of 2006 safeguards the following human rights and freedoms:

[67] Law on Information Security

- *Article 23. Dignity and the free development of individuals*
- *Article 40. Inviolability of home*
- *Article 41. Confidentiality of letters and other means of communications*
- *Article 42. Protection of personal data*
- *Article 43. Freedom of thought conscience and religion*
- *Article 46. Freedom of thought and expression*
- *Article 51. Right to information*
- *Article 54. Freedom of assembly*
- *Article 55. Freedom of association*
- *Article 64. Rights of the child*
- *Article 90. Protection of consumers (against health, security, privacy and dishonest activities)*

187. Serbia has not adopted specific legislation on human rights online; however, several stakeholders pointed out that both constitutional and ordinary courts protect human rights equally in offline and online settings. Serbia is a signatory of multiple international treaties on human rights, such as (i) International Covenant on Civil and Political Rights, (ii) International Covenant on Economic, Social and Cultural Rights, (iii) the European Convention on Human Rights and Fundamental Freedoms and its Protocols, (iv) the Revised European Social Charter, and (v) U.N. Conventions, such as the Geneva Convention relating to the Status of Refugees, the Convention against Torture, the Convention on the Rights of Persons with Disabilities, the Convention on the Rights of the Child, the Convention on the Elimination of All Forms of Discrimination against Women and the Convention on the Elimination of All Forms of Racial Discrimination. Also, standards established by the jurisprudence of the U.N. Human Rights Committee and the European Court of Human Rights are binding for Serbia.

188. According to the 2018 Human Rights Report provided by the U.S. Department of State, there were no reports that the Serbian government restricted or disrupted access to the Internet, monitored private online communication without appropriate legal authority, or censored online content.[68]

189. As noted above, the Constitution of Serbia recognises personal data protection as a constitutional right in the following manner:

> *"Protection of personal data shall be guaranteed. Collecting, keeping, processing and using personal data shall be regulated by the law. Use of personal data for any the purpose other the one were collected for shall be prohibited and punishable in accordance with the law, unless this is necessary to conduct criminal proceedings or protect the safety of the Republic of Serbia, in a manner stipulated by the law. Everyone shall have the right to be informed about personal data collected about him, in accordance with the law, and the right to court protection in case of their abuse."*

[68] U.S. Department of State (2018) Serbia 2018 Human Rights Report. https://www.state.gov/wp-content/uploads/2019/03/SERBIA-2018-HUMAN-RIGHTS-REPORT.pdf

190. In 2005, Serbia ratified the CoE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108),[69] and in 2008 one of its two additional protocols.[70] Serbia adopted the current Law on Personal Data Protection (LPDP) in November 2018 (which entered into force in August 2019) to harmonise the national legal framework with the EU laws required by the Stabilization and Association Agreement (Article 81).[71] Some stakeholders pointed out that the LPDP exceeds the standards established by the EU General Data Protection Regulation (GDPR). It was noted that some stakeholders consider that LPDP still needs to be strengthened in certain areas (e.g. video surveillance).

191. As part of the harmonisation process, the Commissioner for Information of Public Importance, established under the Law on Free Access to Information of Public Importance ("Official Gazette No. 120/04 and 54/07) also acquired a function of the data protection authority in Serbia, becoming the Commissioner for Information of Public Importance and Personal Data Protection (DPA) -Article 59 LPDP.

192. On the website of the DPA (https://www.poverenik.rs), the general public can access useful information, such as annual reports, manuals, videos, guidelines related to the personal data protection framework and DPA's powers and functions. As part of the LPDP dissemination process, DPA has organised multiple training sessions with different stakeholders, including private sector organisations. DPA, as a regulatory body, still needs to strengthen some specific areas to adequately enforce the LPDP, such as more training for its staff members.

193. There is no general law on child protection; nor is there a specific law on child online protection in Serbia. However, there are some regulations and laws which regulate issues related to children online protection:

    a. ***Law on Information Security – article 19a*** (2016).[72] This article states "A Competent Authority shall undertake preventive measures for safety and protection online, as well as public interest activities, by educating and informing citizens, especially children, parents and teachers, about advantages, risks and ways of safe use of the internet …".

    b. ***Regulation on the Safety and Protection of Children in the use of ICT*** *(2016)*.

    c. ***Law on Special Measures for the Prevention of Crime against Sexual Freedom Involving Minors*** (2013). This law applies to those individuals who commit the following offences against minors: rape, sexual intercourse with a defenceless person, sexual intercourse with a child, sexual abuse of power, illegal sexual activities, procuring and facilitating sexual intercourse, acting as a go-between in prostitution, showing, obtaining and owning pornographic material and exploitation of a minor in pornography, persuading a minor to witness sexual

[69] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=283oQoXU

[70] https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7834785

[71] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2013:278:FULL&from=en

[72] https://www.ratel.rs/uploads/documents/empire_plugin/5e9f4832cdb97.pdf

activity, abusing the Internet or other means of communication to violate the sexual autonomy of a minor.[73]

d. ***Criminal Code*** (2005). This law has a number of criminal sexual offences in which ICT means are used to exploit and abuse children (Article 178-186, 388) such as child pornography online[74] and grooming online (Article 185b).[75]

e. ***Law on Electronic Commerce*** (2009). Article 20(2) states that ISPs are compelled to report to the competent authorities any 'illegal activities', including child pornography cases.

194. In 2017, MTTT established the ***National Contact Centre for Children's Safety on the Internet*** as a unique body to conduct counselling for children, parents, students and teachers, as well as other citizens, about the advantages and risks of using the internet and promoting safe ways to use new technologies. This Centre equally receives reports about harmful, inappropriate and illegal content and behaviour on the Internet which violate children's rights (https://www.pametnoibezbedno.gov.rs). MTTT also organises the "IT Caravan" every year, which is an educational campaign promoting the useful, creative and safe use of information technologies. The IT caravan is part of the ***"Smart and Safe"*** platform, which promotes the advantages of using the internet and new technologies in education, business and communications, as well as the dangers resulting from their improper use.[76]

195. Even though Serbia has taken a number of actions to protect children online, some participants from NGOs argued that those actions should address this issue in a comprehensive manner. It was noted that awareness-raising campaigns and education at a school level have to be strengthened so that children clearly understand which steps should be followed to report grooming, cyberbullying, child pornography and other similar offences.

196. Serbia has also ratified international treaties such as the U.N. Optional Protocol to the Convention on the Rights of the Child on Sale of Children, Child Prostitution and Child Pornography (2002);[77] CoE's Convention on Cybercrime -Budapest Convention- (2009) and CoE's Convention on Protection of Children against Sexual Exploitation and Sexual Abuse -Lanzarote Convention- (2009).

197. The Constitution of Serbia in its article 90 states that "… [t]he Republic of Serbia shall protect consumers. Activities directed against health, security and privacy of consumers, as well as all other dishonest activities on the market, shall be strictly prohibited."[78] There is also a general Law on Consumer Protection (2014), which sets

[73]https://www.ohchr.org/Documents/Issues/Children/SR/CareAndRecovery/Serbia.doc

[74]https://rm.coe.int/serbia-appendix-lanzarote-2nd-monitoring-round/168076f44c+&cd=2&hl=en&ct=clnk&gl=cr

[75] International Centre for Missing and Exploited Children (2017) Online Grooming of Children for Sexual Purposes.https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf

[76]https://www.betterinternetforkids.eu/web/serbia/sid

[77]https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=154&Lang=EN

[78]http://www.parlament.gov.rs/upload/documents/Constitution_%20of_Serbia_pdf.pdf

out the fundamental rights of the consumers, conditions and means of consumer protection, rights and responsibilities of the consumer protection organisations, establishment of the system of out-of-court settlement of consumer disputes and the rights and responsibilities of the state institutions in the area of consumer protection (article 1). This law regulates rigorously unfair commercial practices in the country, including those practices related to e-commerce transactions (articles 19 and 20).

198. The Law on Consumer Protection created the **National Council for Consumer Protection** (article 126), under the aegis of the MTTT, to strengthen the system of consumer protection and cooperation of the bodies, organisations and other institutions in charge of consumer protection in the country. It was noted that there is no department within the MTTT dealing with consumer protection online.

199. In a 2019 European Commission Staff Working Document, it was stated the following recommendations:

> *"*Better cooperation mechanisms between the line ministries and consumer organisations need to be established. Similarly, cooperation among consumer protection organisations remains fragmented and requires improvement. The authorities' administrative capacity for consumer protection and the inspection services in charge of consumer protection, product safety and non-safety related issues need further strengthening. The institutional setting and protection of consumer protection rights and interests at the local level require improvement. Unfair commercial practices and contract terms need to be addressed, and vulnerable consumers need to be protected."[79]

200. In July 2019, the National Assembly of the Republic of Serbia adopted a new Law on Trade and some amendments to the Law on Electronic Commerce (2009) to be fully harmonised with the EU laws. The Law on Electronic Commerce establishes some provisions regarding consumer protection on cross-border services, the validity of electronic contracts, responsibility of service providers, and several fines and penalties for unfair practices. The Law on Trade introduces new concepts which define the online store and online platform for the first time in the Serbian legislation.[80]

201. Serbia has adopted a comprehensive intellectual property legal framework which covers patents, copyrights, trademarks, industrial designs, topographies of semiconducting products, trade secrets and other matters.[81] One of those laws -the Law on Protection of Copyright and Related Rights (2009)- regulates the protection of the rights of the authors of literary, scientific and artistic works, and related rights, including the judicial protection of them. This law was recently amended to be a step closer to international and EU intellectual property standards. The recent changes implied, *inter alia*, an increase in the level of protection of performers, authors of software and database producers.[82]

202. The Serbian Criminal Code also establishes some criminal offences against intellectual property, such as "Violation of Moral Rights of Author and Interpreter" (article 198),

[79] https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-serbia-report.pdf
[80] http://www.zslaw.rs/new-law-on-trade-and-amendments-to-the-law-on-electronic-commerce-adopted/
[81] http://www.zis.gov.rs/legal-regulations/laws-and-regulations.110.html
[82] http://www.zslaw.rs/adoption-of-the-amendments-to-the-serbian-ip-laws-a-step-closer-to-reaching-eu-standards/

"Unauthorised Use of Copyrighted Work or Item Subject to Related Right" (article 199), "Unauthorised Removal or Change of Electronic Information on Copyright or Similar Rights" (article 200), "Violation of Inventor's Rights (article 201), and "Unauthorised Use of Another Person's Design" (article 202). At the international level, Serbia has ratified several treaties, including the WIPO Copyright Treaty (2003)[83] and the WIPO Performances and Phonograms Treaty,[84] which are known as the 'Internet Treaties'.

203. The Criminal Code of Serbia establishes the following substantive provisions related to cybercrime offences:

- Article 298: Damage to Computer Data and Programs
- Article 299: Computer Sabotage
- Article 300: Developing and Entry of Computer Viruses
- Article 301: Computer Fraud
- Article 302: Unauthorised Access to Protected Computer, Computer Network and Electronic Data Processing
- Article 303: Preventing and Constraining Access to Public Computer Network
- Article 304: Unauthorised Use of Computer or Computer Network
- Article 304a: Making, Procuring and Providing to Another Person Means for Committing Criminal Offences against Security of Computer Data

204. Similarly, procedural cybercrime legislation is established in the Criminal Procedure Code under the following provisions:

- Article 147: Temporary Seizure of Objects
- Article 148: Duty of a Holder of an Object
- Article 152: Search
- Articles 166-168: Convert Interception of Communications
- Article 178: Computer Date Search
- Article 179: Order on Computer Data Search
- Article 180: Implementation of Computer Data Search
- Article 282: Actions to be taken by the Public Prosecutor upon receiving a criminal complaint

205. The Law on Electronic Communications also provides a couple of procedural provisions:

- Article 127: Lawful Interception of Computer Data
- Article 128: The Obligation to retain data (for 12 months)

[83] https://www.wipo.int/treaties/en/notifications/wct/treaty_wct_43.html
[84] https://www.wipo.int/treaties/en/notifications/wppt/treaty_wppt_43.html

206. As noted above, Serbia has ratified and implemented the CoE's Convention on Cybercrime (Budapest Convention), including its Additional Protocol on Xenophobia and Racism Committed through Computer Systems.

207. Despite the national legislation on cybercrime, electronic evidence and search, seizure and confiscation of online crime proceeds was strengthened considerably in the recent years, the CoE, in a recent assessment report, revealed that further reforms are needed to allow effective cybercrime investigations and prosecution in the light of the latest technological developments, as well as the fast-changing pace of the *modus operandi* of cybercrime.[85]

208. Some government stakeholders recognised the above situation and also pointed out that the Ministry of Justice created a Working Group, which is presently working on the implementation of the action plan to comply with SAA Chapters 23 (Judiciary and Fundamental Rights) and 24 (Justice, Freedom and Security). As part of this harmonisation process, it was noted that both the Criminal Code and the Criminal Procedure Law would be slightly amended (mainly the procedural cybercrime provisions) to be fully in compliance with the EU laws.

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: Established

209. In 2005, Serbia adopted the Law on the Organisation and Jurisdiction of Government Authorities for Combating Cybercrime (LOJGA) as part of the process of strengthening the legislative and institutional framework of the Judicial System. This law was passed to regulate the creation, organisation, competencies and powers of special organisational units of government authorities which handle the investigation, detection, prosecution and trying of criminal offences, including cybercrime offences, specified in the law (articles 1 and 3 LOJGA).

210. LOJGA also established and defined the responsibilities and functions of the three main government bodies directly related to the investigation, prosecution and process of cybercrime cases in Serbia: (1) the Cybercrime Unit, (2) the Special Prosecutor's Office, and (3) the Higher Court in Belgrade, which was designated as the competent court to try, among other cases, cybercrime offences for the entire country.

211. Some stakeholders pointed out that the Cybercrime Unit was created in 2007 under the aegis of the Police Department, MoI (article 9 LOJGA). The Cybercrime Unit will

[85] https://www.coe.int/en/web/cybercrime/-/iproceeds-assessment-of-legislation-on-cybercrime-and-e-evidence-in-serbia

proceed with any investigation at the instance of the Special Prosecutor, per article 9 LOJGA.

212. Currently, the Cybercrime Unit has a staff of 23 members. As part of the Chapter 24 negotiations, the staff of this Unit has almost tripled in the last decade. It was noted that these staff members are trained continuously, both locally and internationally, the latter mainly by international organisations. For instance, some officers had been sent to the UK for a specialised training and some staff members also earned the MSc in Forensic Computing and Cybercrime Investigations from the University College Dublin. It was noted that training standards and policies have been implemented; however, capacity building needs to be strengthened, as well. It was noted, for example, that skilled staff rotation has become an issue within the Cybercrime Unit. It was also said that this Unit is well-equipped, but financial resources are limited.

213. Even though the digital forensics activities are conducted by a separate agency within the Police Department, it was said that the digital chain of custody and evidence integrity protocols and procedures have been established and are rigorously followed to ensure that the collected digital evidence is admitted by the court. The Cybercrime Unit and other units (IT Forensic Unit) within the Police Department understand clearly what their roles and responsibilities within the cybercrime investigative process are. It was also noted that the financial and human resources of the IT Forensic Unit have to be strengthened.

214. This Cybercrime Unit is not only focused on cybercrime investigations; it has also engaged in awareness-raising campaigns (e.g. child online protection). This Unit has also established effective collaboration channels with international law enforcement agencies, such as FBI, the UK Police, EUROPOL, amongst others. The Cybercrime Unit works closely with the national CERT, the Association of Serbian Banks, the Financial Investigation Unit and other public and private sector organisations.

215. The Higher Prosecutor's Office established in 2006 the Special Prosecutor's Office (article 4 LOJGA) to prosecute the offences described in article 3 LOJGA, which includes the cybercrime offences prescribed in the Criminal Code. The Special Prosecutor's Office is competent to prosecute those criminal offences for the entire territory of the Republic of Serbia.

216. Some stakeholders pointed out that the Special Prosecutor's Office has a total of 23 prosecutors who handle not only cybercrime cases but also intellectual property and other offences. However, only six prosecutors are specialised in cybercrime matters; those prosecutors are still considered limited in quantity to cover the entire country. It was noted that the staff members of the Special Prosecutor's Office are trained, both locally and internationally. Some stakeholders pointed out that those six prosecutors are experienced enough to investigate and prosecute complex cases and cross-border cybercrime cases.

217. Some stakeholders pointed out that the Special Prosecutor's Office faces some challenges, such as limited training opportunities, financial constraints and its equipment is rudimentary. Other participants highlighted that international cooperation and information-sharing mechanisms should be strengthened, and the coverage of the public awareness-raising campaigns should be expanded to facilitate the Special Prosecutor's Office's work.

218. The Special Prosecutor's Office maintains records and statistics on the number of cybercrime cases in Serbia. It was noted that those figures have substantially

increased since its foundation,[86]thus the capacity of the staff members of the Special Prosecutor's Office has to be strengthened, by investing in more financial, technological, and human resources, to keep pace with the current cybersecurity landscape.

219. In 2017, the Special Prosecutor's Office established a cooperation arrangement with Save the Children, an international organisation, within a Judicial Academy programme to develop training programmes for judges and public prosecutors in the field of cybercrime and child online protection. As part of this programme, some experts in the field prepared a *"Guide for Judges and Prosecutors on Cybercrime and Child Online Protection in the Republic of Serbia*". This document contains clear guidelines for prosecutors and judges, including electronic evidence, international standards in this field, domestic legal and institutional framework, as well as the protection of children in criminal proceedings.[87]

220. The Special Prosecutor's Office is working closely with the CoE and the EU through the Global Action on Cybercrime+ (GLACY+) programme, which aims at implementing the Budapest Convention and providing direct administrative and technical assistance to the countries that are covered by this specific programme.[88]

221. The Higher Court in Belgrade established a Cybercrime Department to proceed in cases involving those criminal offences set in article 3 LOJGA (article 11 LOJGA). The Higher Court has the first-instance jurisdiction in cybercrime matters, and the Appeals Court in Belgrade has the competent jurisdiction to proceed in the second instance (article 10 LOJGA).

222. Some stakeholders pointed out that the Higher Court in Belgrade has a total of 17 judges, of which only a few judges are specialised in cybercrime offences and electronic evidence. It was noted that those judges are regularly trained, both locally and internationally, by international organisations, such CoE, OSCE, among others. However, the delivery of capacity building needs to be strengthened. It was said that the Cybercrime Department has adequate equipment to deliver the services, but its financial resources are limited.

223. From the Criminal Justice System perspective, Serbia has committed to harmonising the domestic legislation with the EU laws and directives and adopting a number of measures, which are described in the Action Plan of Chapter 24, such as the improvement of the institutional, human and technical capacities to combat cybercrime in Serbia.

224. According to the National Cybercrime Strategy 2019-2023, those actions are led by the MoI and have several activities oriented to enhance the capacity of the bodies mentioned above, such as:

- Reorganisation of the Department for the Suppression of Cybercrime
- Creation of special organisational units in relevant bodies and organisations in compliance with their competencies and needs

[86]https://rm.coe.int/t-cy-2018-36-item5-compilation-of-replies/16808f1f74
[87]https://rm.coe.int/t-cy-2018-36-item5-compilation-of-replies/16808f1f74
[88]https://rm.coe.int/t-cy-2018-36-item5-compilation-of-replies/16808f1f74

- Improvement of personnel, professional, technical and organisational capacities of the competent institutions for the exchange of information on cyber incidents
- Implement the necessary training at different levels
- Procure cutting-edge electronic equipment, software and tools
- Harmonisation of standards and operating procedures of the bodies responsible for combating cybercrime

225. As noted above, the institutional capacity to investigate, prosecute and try cybercrime cases have been established, but it still needs to be strengthened in different areas. The Government is aware of this situation and is currently taking some actions to improve the criminal justice system as a whole.

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

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.

Stage: Established

226. It was noted that formal mechanisms of international cooperation have been set out in order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution with established communication channels. Serbia has also established cooperation arrangements with NATO, EU, CoE, Interpol and Europol, OSCE and other international organisations, as well as bilateral agreements with other countries on cross-border information sharing and cybercrime matters (e.g. India, Russia). Mutual legal assistance and extradition agreements[89] (e.g. Croatia, Montenegro, North Macedonia, USA) have been established, which also apply to investigation and prosecution of cybercrime cases. In 2016, the Government and civil society institutions signed a cooperation agreement to combat cybercrime in the country.

227. Legislative requirements for the exchange of information between domestic public and private sectors have been established. The Law on Information Security obliges certain actors, such as the national CERT, the operators of ICT systems of Special Importance, amongst others, to exchange information on cyber incidents, vulnerabilities, threats, etc. Law Enforcement agencies and other regulatory bodies also have formal agreements in place on information sharing.

228. Serbia expressly recognised in the SDIS that domestic and international cooperation and information sharing (as guiding principles) are fundamental to enhance the cybersecurity capacity of the country:

[89] https://rm.coe.int/serbia-revised-template-extradition-en-2018/16808cce9e

- "… [e]stablish continuous cooperation between the public and the private sector as a basis for development and improvement of strategic priorities …" and,
- "…[i]t is necessary to establish and improve regular and efficient exchange of information on risks and incidents in the field of information security, at the national and international levels …".

229. It was also noted that informal relationships between the Government and criminal justice actors (Cybercrime Unit, Special Prosecutor's Office and Judges) have been established, resulting from regular information-sharing mechanisms.

230. It was also noted that effective informal cooperation mechanism between ISPs and law enforcement agencies have been established with clear channels of communication.

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 Serbia. 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 Set mechanisms in place to review the cybersecurity legal and regulatory framework to identify where gaps and overlaps may exist and amend or enact new laws accordingly to reflect changes in national priorities and the international ICT and cybersecurity landscape.

R4.2 Set mechanisms in place for continuously harmonising the cybersecurity legal and regulatory framework with national cybersecurity-related policies and strategies, the EU laws required by the Stabilization and Association Agreement (Chapters 23 and 24), international and regional treaties, international standards and good practices. Allocate sufficient resources to ensure full enforcement of existing and new cybersecurity and cybercrime-related laws and regulations and monitor their implementation.

R4.3 Ensure that international and regional trends and good practices inform the assessment and amendment of domestic legal and regulatory frameworks *protecting human rights online*, *personal data protection, child online protection*, *consumer protection online*, and *intellectual property online*.

R4.4 Designate, within MTTT's trade division, a lead agency or body responsible for the protection of consumer online with sufficient human, technological and financial resources to operate as such.

R4.5 Revise the Criminal Code, Criminal Procedures Code and any other domestic legal instruments to ensure that the current substantive and procedural criminal provisions and international cooperation provisions to combat cybercrime in Serbia (1) exceed minimal baselines specified in international standards, (2) respond to the fast-paced environment, and (3) provide adequate mechanisms and instruments to successfully conduct the investigation, prosecution and trying of complex and cross-border cases.

CRIMINAL JUSTICE SYSTEM

R4.6 Invest in advanced investigative capabilities to allow the investigation of complex and cross-border cybercrime cases, supported by regular testing and training of law-enforcement investigators.

R4.7 Strengthen national investigation capacity to adequately investigate cybercrime cases in Serbia, including sufficient human, financial and technological resources.

R4.8 Ensure that the law enforcement agencies maintain the integrity of collected data and evidence to meet international evidential standards in cross-border investigations and also collect and analyse statistics and trends on cybercrime investigations.

R4.9 Expand funding for law enforcement hiring (if needed) and training, both locally and internationally, to dive into more sophisticated and specialised matters based on their priorities and needs.

R4.10 Strengthen national prosecution capacity to adequately investigate and prosecute cybercrime offences in Serbia, including sufficient human, financial and technological resources. Ensure that the statistics and trends on cybercrime prosecution are collected and analysed.

R4.11 Expand funding for prosecutor's office hiring (if needed) and training, both locally and internationally, to dive into more sophisticated and specialised matters based on their priorities and needs.

R4.12 Establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.

R4.13 Expand funding for judges' hiring (if needed) and training, both locally and internationally, to dive into more sophisticated and specialised matters based on their priorities and needs. Ensure that judges who are trying cybercrime cases, and the whole department, have sufficient financial, technological and human resources to perform the assigned tasks and functions.

R4.14 Develop and institutionalise specialised training programmes for law enforcement officers, prosecutors and judges on cybercrime and electronic evidence through the CoE's GLACY+ programmes or other training programmes.

R4.15 Building formal cooperation mechanisms between the national CERT and other sectors, including CI/CII sectors, on collecting and analysing cyber incidents thought an information-sharing platform.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.16 Ensure that the existing international cooperation mechanisms are fully functional, and that the channels of communication are established. Also, expand and enhance formal cooperation mechanisms to combat cybercrime as needed.

R4.17 Allocate resources to support the exchange of information between public and private sectors domestically and enhance legislative framework and communication mechanisms.

R4.18 Strengthen informal cooperation mechanisms between domestic and foreign Internet Service Providers and law enforcement with clear communication channels to combat cybercrime.

R4.19 Strengthen formal cooperation mechanisms between domestic law enforcement agencies with foreign counterparts on cross-border cybercrime investigations and prosecutions.

R4.20 Strengthen informal cooperation mechanisms between government agencies and criminal justice actors to exchange information on cybercrime issues.

DIMENSION 5 STANDARDS, ORGANISATIONS AND TECHNOLOGIES

231. 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: Formative to Established

232. ICT Security standards and good practices have been adopted by institutions in both the public and private sectors, and the Law on Information Security, adopted in 2016, identifies a series of actions for the protection of critical systems, called "systems of special importance", that constitute a baseline for public and private sector operators to follow. Furthermore, according to this law, each operator of a system of special importance must create internal policies and procedures, encoded in an "act", that determine "the protection measures, and in particular the principles, method and procedures to achieve and maintain an adequate level of system security, as well as the powers and responsibilities related to the security and resources of the ICT system of special importance". In addition, the act obliges each of these operators to annually conduct, and report on the status of, compliance with the measures described in the law to an appropriate government entity. With regards to the ICT Systems of Special Importance, there is a further regulation titled "On More Detailed Regulation of Measures of Protection of Information and Communication Systems of Special

Significance"[90]. This regulation, which contains more than 30 articles, describes the processes the operators of these systems must comply with. For example, article 2 addresses the organizational structure operators must create to manage its information security environment, including the roles and responsibilities of employees.

233. While the Law on Information Security and the additional regulation mentioned above requires adoption of measures of protection, it does not prescribe any specific standard that organizations must use. However, discussions with government representatives revealed that the additional regulation is largely modelled on the ISO 27001 standard. Furthermore, many government entities are currently engaged in, or exploring, the adoption and certification according to the ISO 27001 standard. It was noted that the Law was drafted partially based on elements of the ISO 27001 standard as well as the National Institute of Standards and Technology (NIST) framework, and some government entities indicated that their internal policies were based on SANS top-20 and the NIST framework. While many ministries appear to be pursuing adoption of the ISO standard, it also appears that they are doing so in isolation from each other. Better coordination and alignment across all of government, with both the standard as well as on policies and practices, might result in a more consistent application of the standards and policies, while possibly achieving economies of scale.

234. Within the private sector the adoption and certification of the ISO 27001 standard was prevalent, particularly within the financial industry. It was noted that although the financial regulator did not prescribe a particular standard, representatives participating in the assessment focus groups claimed possession of the ISO 27001 certification. However, at least one private sector entity in the financial industry indicated that they were unsure of the value of obtaining the certification, given the expense required to achieve it. They felt that there was very little competitive advantage to completing the certification, and that implementing components of the standard may, in principle, achieve the same result. Nevertheless, the ISO standard is found to be in use across the industry, and the financial regulator reported that they monitor compliance with the standard.

235. In other industries, implementation of the ISO standard was less consistent. Some internet companies noted that they do not follow the ISO standard, but nevertheless adhere to requirements imposed by other bodies, such as the Internet Corporation for Assigned names and Numbers (ICANN), as well as other data communication coordinating entities. Representatives of the government that work closely with the private sector on digital development plans reported that medium and large-scale enterprises are committed to enhancing their cybersecurity posture. They note there is only limited interest in the ISO standard, but instead implement a set of measures and procedures that align with their requirements. Furthermore, many of these companies note that customers and business partners are increasingly requiring the establishment of cybersecurity policies and practices in order to conduct business.

236. Those organizations that have implemented cybersecurity standards and good practices guiding procurement indicated that they do so mainly through the relevant components of the ISO 27000 standard. Several of the financial entities indicated that clearly defined procedures for technology procurement existed, including specific requirements for bidders. The government maintains a portal for the public procurement of goods and services, and the while the government's public

[90] https://mtt.gov.rs/en/download/r5.pdf

procurement office[91] has the responsibility of overseeing procurement in the public sector, the Office of ICT is responsible for providing an opinion to the State Audit Institution on the procurement of information and communication equipment and software solutions procured by state administration bodies and government departments. Standardization is implemented through this process; while the Office does not prepare the specification of the equipment procured by the authorities, it provides support for determining the optimal resources required for the performance of each department's operations.

237. The situation for software development standards is similar to procurement standards in that only a few participants from all sectors indicated any specific standards in this area. However, it was noted that software development, in general, is a growing field in Serbia[9293], and therefore it is common for developers to confer in the latest trends and adhere to international good practices, including in secure software development. Other participants concurred indicating that while they may not have adopted specific, internationally-recognized standards in their institutions, they had adopted practices that support the development of secure 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: Established

238. While Serbia, with a World Economic Forum network readiness index of 55, falls approximately midway in the 139-country survey, it lands higher than midway in its infrastructure (48) and affordability (56) scores. The experience of the CMM team is that at least in the urban centre of the capital, the Internet is reliable and affordable, and stakeholders universally concur that Serbia's Internet services and infrastructure are well-established and reliable, and by all appearances managed to international IT guidelines, standards, and good practices. According to one participant: *"I have been working in telecommunications [in Serbia] for 31 years and as far as I remember everybody is always working with a certain level of redundancy; I never seen that here in Serbia telecommunications operators install systems without any level of redundancy."*

239. There are a number of both terrestrial and mobile broadband operators, and access to the global Internet is through multiple connections around the country, each

[91] www.ujn.gov.rs

[92]https://www.digitalknights.co/blog/dissecting-serbia-nations-outsourcing-important-good

[93]https://www.reuters.com/article/us-serbia-tech/serbia-turns-to-tech-industry-to-fight-economic-stagnation-idUSKBN1L117Z

managed by a different ISP. A 2015 study[94] by RIPE showed 13 pathways from Serbia[95]. The telecommunications regulator, RATEL, licences all ISPs but only through notification: i.e. they only require notification of the creation of a new ISP business. In its 2017 annual report, RATEL recorded 194 "Internet Access and Internet Services" operators. Participants also noted that there are seven root DNS servers in the country, further enhancing Internet reliability.

240. To oversee the operations of ISPs, RATEL adopted its "Rulebook on general terms and conditions for performing electronic communication activity under general authorization regime (*Official Gazette of the Republic of Serbia no. 58/18*)"[96]. This document outlines the requirements for operators and the role of RATEL in ensuring the resiliency of electronic communications in the country. Article 2 of the Rulebook establishes that the quality parameters described are based on international standards, including those of the "European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), Internet Engineering Task Force – Request for Comments (IETF- RFC), as well as the standards, decisions and recommendations of the International Telecommunication Union (ITU), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and the European Conference of Postal and Telecommunications Administrations (CEPT) (hereinafter referred to as international standards) and relevant national standards". The rulebook also includes the requirements for operators to collect relevant information and perform measurement and testing at least annually, with additional controls conducted on the request of RATEL.

241. The internet is used extensively for e-commerce and e-government (see D2.2), and web site security is frequently deployed. Authentication processes for access to secure web sites are well-established, however participants noted that only a few places, mostly financial institutions, utilize two-factor authentication.

[94] https://labs.ripe.net/Members/emileaben/measuring-countries-and-ixps-in-the-see-region

[95] While not a detailed analysis of traffic into and out of Serbia, it is an indication of the redundancy of the Internet in the country.

[96] https://www.ratel.rs/uploads/documents/pdf_documents/documents/Regulativa/Pravilnici/Telekomunikacije/Rulebook%20on%20quality%20parameters%20for%20publicly%20available%20electronic%20communication%20services.pdf

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: Formative

242. As with many aspects in this dimension, the environment for software quality can vary considerably depending on the institution and industry. The financial sector is leading in this area, with many firms reporting the existence of white-lists for software and a controlled installation and update environment, including rigorous testing of new software versions. Within the government it was noted that a list of approved software is under development, but also noted that workstations are secured so that software installation can only be performed by a system administrator. In the private sector, major companies are reported to generally manage their software according to the policies and standards they have adopted, but smaller business do not usually perform these types of tasks. As noted in factor 5.1 on software standards, Serbia has a rapidly developing software development industry, with global software companies investing heavily in the country. It was noted that these companies, as well as the smaller software development businesses, routinely monitor their software for defects. Searches on several Serbian employment web sites reveal many jobs and freelancers available for software quality assurance tasks, indicating that software quality deficiencies are being gathered and assessed.

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: Formative

243. Up-to-date technical security controls are deployed in all sectors of Serbia, although the level of implementation can vary depending on the sector or size of the establishment. In the public sector, government entities interviewed noted it was a standard practice to apply controls such as automatic software patching and anti-virus updating, firewall management, offsite storage of backups and physical security controls, as well as some limited use of intrusion detection systems. Some government representatives also noted that the networks are monitored for unapproved devices and workstations are secured so that users are unable to install unapproved software. Furthermore, the additional regulation noted for aspect 5.1 above includes requirements for many technical security controls for the operators of

ICT system of special significance. For example, article 13 calls for the implementation of physical protection of facilities, article 15 addresses backup procedures and article 16 requires the "means … for detecting malware and removing damages caused by malware…".

244. According to participants, a similar environment exists in the private sector, although the variation in deployment is much greater. Financial, telecommunications and larger institutions deploy a much broader range of controls and exhibit a much deeper knowledge not only of the importance of these controls, but also have the skills and financial resources to deploy them. It was noted that mid-sized, and some smaller, enterprises outsource their ICT operations, and therefore depend on their provider to ensure the security of the environment. During the focus group discussions this was represented as an advantage, and there was agreement that most of these service providers would perform security functions, including network monitoring for intrusion detection, server software patching, backups and physical security of the information technology infrastructure. Representatives of these service providers concurred that hosted systems usually included software patching, backup and other related security services as part of their regular services. Some of the ISPs, including Telecom Serbia, the largest provider of fixed and mobile Internet access in the country, report the use of antivirus and antispam as a regular component of the e-mail product offering.

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: Established

245. The use of cryptographic controls in Serbia is well understood, deployed and mandated. Article 7 of the Law on Information Security includes 28 protection measures for ICT systems of special importance, with measure 11 calling for system owners to provide "the appropriate use of crypto protection in order to protect data secrecy, authenticity and/or integrity". Furthermore, the Law on Information Security, in section "IV. Cryptosecurity and Protection against Compromising Electromagnetic Emanations" address the oversight and use of cryptographic products.

246. Consultations with stakeholders from both the public and private sector institutions indicated knowledge of the need for encryption of data - both at rest and in transit. Participants noted that encryption had been applied to selected systems in use, and an online review of government and private sector web sites revealed that these routinely utilized SSL/TLS services. Financial institutions, in particular, highlighted their application of cryptographic processes for all systems, especially payment systems. Other businesses noted their frequent application of encryption at the workstation level. Telecommunications operators also indicated the extensive use of encryption. Finally, participants agreed that Serbia has a long tradition of the use of cryptographic technologies, with several companies, either based in Serbia or have

product development teams in the country, engaged in the development and marketing encryption products[97].

D 5.6 CYBERSECURITY MARKETPLACE

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

Stage: Formative to Established

247. While not a major component of the Serbian economy, the ICT industry in Serbia is growing substantially. According to some reports, "the Serbian ICT industry generated 913 million euros worth of exports during the first eight months of the year, a 26.4 per cent increase compared with the corresponding period of 2018". According to participants, even though ICT as a business sector is growing, the focus is mainly on software development for business applications. However, there is also a growing cybersecurity marketplace with several Serbia-based companies creating cybersecurity products. Examples include Towers Net Beograd[98], which includes network intrusion detection systems among its product offerings, and AST[99], which provides cybersecurity monitoring services, as well as local importers and distributors for most of global security appliance manufacturers. Furthermore, participants mentioned a Serbian company developing solutions, such as custom honeypot products, primarily for the Asian market, and other participants noted some awareness of companies working on customizing cybersecurity solutions. In addition, many of the global technology companies (IBM, Cisco, et. al.), global consulting companies (KPMG), and local companies[100] offer cybersecurity services to the local market.

248. Very little information on a cybersecurity insurance market was available from participants or through online research. Some participants noted that these products are available on request from insurance companies, although they were not viewed as necessary or important.

[97] See as examples http://www.towersnet.rs/products/encryption/, https://www.verisec.com/about-verisec/verisec-labs/

[98] http://www.towersnet.rs

[99] https://www.ast.co.rs

[100] https://ras-it.rs, https://solvit.rs,

D 5.7 RESPONSIBLE DISCLOSURE

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.

Stage: Formative to Established

249. The Law on Information Security and the Law on Electronic Communications both have mandatory disclosure requirements for operators and together provide a framework for disclosure of security incidents. In the case of the Law on Information Security, Article 11 obliges the operators of ICT systems of special importance to "inform the Competent authority about incidents in ICT systems that can have a significant impact on information security breaches". This article also explicitly requires other institutions to notify competent authorities of incidents; financial institutions notify the National Bank of Serbia; telecommunications operators to the telecommunications regulatory authority; and operators of ICT systems dealing with classified information in accordance with their specific regulations.

250. The Law on Electronic Communications also includes a disclosure component. Article 124 of the law, in section XVI on Security and Integrity of Public Communications Networks and Services requires operators of public communication networks and services to notify subscribers of any risks related to the violation of these facilities. Article 125 of the law requires operators to notify the telecommunications regulator. Since the assessment in 2019, and during the report preparation and review process, Serbia enacted further legislation in early 2020 specifying procedures for notification of incidents. This act, titled "On the incident notification procedure in information and communication systems of special importance", lays out in detail the procedures, roles and responsibilities for analysis, reporting and sharing of incident information amongst the operators of ICT systems of special importance.

251. A number of CERTs operate in the Serbian ecosystem. The national CERT, operating under the authority of the telecommunications regulator RATEL, acts as a coordinating mechanism, while the government has a central CERT that serves most government departments. Four other government entities operate independent CERTs[101]. In addition, several other non-government CERTs are registered with the National CERT[102]. While the legislation mentioned above specifies some reporting requirements, at the time of the assessment, there was no formal requirement for coordination between the CERTs. However, during the assessment report preparation period, an update to the Law on Information Security was published which provides, in article 15a, a procedure for the "National CERT, the CERT OF public authorities and CERTS of independent ICT system operators reflect continuous cooperation" to "… hold joint meetings organized by the national cert at least three times a year, and where appropriate, in the event of incidents having a significant impact on information security … . Furthermore, during the focus group discussions it was noted that a good operating relationship between the CERTs, notably based on the trust

[101] CERT MoD, CERT MoI, CERT MFA and CERT SIA

[102] https://www.cert.rs/en/evidencija-certova.html

development between individuals, results in the coordination and communication between these entities.

252. Finally, the national CERT and MTTT maintain a system for public reporting of incidents as well as an active web site that provides notifications regarding vulnerabilities it believes are useful to communicate. In addition, the web site offers recommendations for actions to take by the general public or businesses to protect their systems.

253. Discussions during the assessment revealed that stakeholders were generally aware of these provisions, but some indicated that, due to a lack of incidents, very few reports were submitted.

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 Serbia. 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 Adopt a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors, including standards in procurement and software development.

R5.2 Further to the recommendation above, consider creating a standard baseline set of security policies and procedures across all government bodies.

R5.3 Further to the recommendation above, appoint a body to assess the level of adoption and compliance with the implemented standards, and create remediation measures based on the results.

R5.4 Further to the recommendation above, publish the results of cybersecurity assessments.

R5.5 Promote the use of cybersecurity standards to the private sector, with a particular focus on small and medium-sized enterprises.

INTERNET INFRASTRUCTURE RESILIENCE

R5.6 Conduct regular assessments of processes according to international standards and guidelines together with assessment of national information infrastructure security and critical services that drive investment in new technologies.

R5.7 Together with all Internet stakeholders, ensure that all processes used to manage and monitor the Internet infrastructure are well documented, with transparent and clear roles and responsibilities.

SOFTWARE QUALITY

R5.8 Complete the software catalogue project currently underway and encourage all critical infrastructure operators to complete theirs. Maintain the catalogue to keep it up to date.

R5.9 Develop policies and processes on software updates and maintenance that is applicable across all government entities and encourage the private sector to do likewise.

TECHNICAL SECURITY CONTROLS

R5.10 Establish consistent policies for technical security control deployment in government and critical infrastructure operators. Regularly monitor the use of these controls and review results with each entity to improve their use.

R5.11 As part of the recommendation above, conduct penetration testing on a regular basis and review enhance the infrastructure based on the results.

R5.12 Promote the use of technical security control frameworks such as the SANS top-20 in the private sector, particularly targeting small and medium-sized enterprises.

R5.13 Consider implementing current standards regarding access control, moving to two-factor authentication where feasible.

CRYPTOGRAPHIC CONTROLS

R5.14 Raise public awareness of secure communication services, such as encrypted/signed emails.

R5.15 Promote the deployment of state-of-the-art tools, such as SSL or TLS, by web service providers, to secure all communications between servers and web browsers. Promotion should be not only to service providers, but target in particular small and medium-sized enterprises and encourage them to insist on these services from their providers.

R5.16 Develop encryption and cryptographic control policies within the public sectors based on previous assessments, and regularly review the policies for effectiveness. Standardize the deployment of these controls across critical infrastructure operators.

CYBERSECURITY MARKETPLACE

R5.17 Building on the growing software development capacity in Serbia, consider promoting the production and marketing of innovative cybersecurity products by domestic producers, for both local use as well as for export.

R5.18 Promote the use of secure coding guidelines, good practices and internationally accepted standards for all software developed in the country, and consider marketing Serbia as a centre of excellence in this area of software engineering.

R5.19 Promote the establishment of a market for cyber-insurance and encourage information-sharing among participants of the market

RESPONSIBLE DISCLOSURE (SEE ALSO THE RECOMMENDATIONS IN DIMENSION 3.2 AND 3.3)

R5.20 While under the current law some operators are required to report breaches, it is also beneficial to establish a framework, starting with critical infrastructure organisations and ISPs, for sharing vulnerability discoveries in order to allow stakeholders to take appropriate mitigation measures before a breach.

R5.21 The framework mentioned above should include the technical details of vulnerabilities. Where possible, such reporting should be in a way that avoids attribution to the reporting entity in order to encourage reporting.

R5.22 Once the framework mechanisms have been stabilized, include other stakeholders, such as product vendors, large and medium-sized companies and academic institutions.

R5.23 Encourage software and service providers to commit to refraining from legal action against a party disclosing information responsibly.

ADDITIONAL REFLECTIONS

254. The CMM team thanks the Ministry of Trade, Tourism and Telecommunications of Serbia for the excellent support provided during the preparation, implementation and follow-up of the assessment, and to all the stakeholders that attended the assessment. The representation and composition of stakeholder groups was comprehensive and balanced, and they all offered insightful contributions. The government of Serbia has clearly made cybersecurity a priority, and the team hopes that stakeholders find the observations and recommendations useful.

The CMM review of Serbia informing this report was conducted in cooperation with the World Bank Group. The Global Cyber Security Capacity Centre (GCSCC) of the University of Oxford contributed to the quality assurance process by reviewing Dimensions 1, 2, 3 & 5. Dissemination of the assessment report is organised in cooperation with the Global Cybersecurity Center for Development (GCCD) under the Korea Internet Security Agency (KISA) of Republic of Korea. Financing for this assessment has been provided by the Korea-World Bank Group Partnership Facility (KWPF) that is administered by the World Bank for South Korea's Ministry of Economy and Finance.