DCAF Geneva Centre
for Security Sector
Governance

National Cybersecurity Strategies in Western Balkan Economies

I Introduction

In the contemporary world, information security is an integral part of overall security and functions to exercise and respect the rights, freedoms and interests of citizens, the economy, and the state. Across the Western Balkan (WB) region, significant progress has been made in developing the information security strategic framework and improving legal and operational capabilities to tackle cyber-related security threats.

The common denominator for these national cybersecurity strategies (NCS) is the integration of similar approaches and compatible structures as defined in the EU NIS Directive, which aims for standardizing terminology, methods, policies and procedures with adopted European and international standards. A commendable effort has been made by all WB economies in developing key strategic documents and legislation based on assessments and analysis of government agencies, local and international organizations, and the private sector, thereby applying comparative methods in terms of best practice alongside using theoretical literature and empirical studies, global trends and practices, and policies of the European Union.

Setting a national cybersecurity strategic and institutional framework can achieve the goal of providing a safe, secure, reliable and resilient digital environment, supported by high-quality capacities, high-quality experts, and built on trust and national and international cooperation in the field of cybersecurity. On the other hand, national cybersecurity strategy priorities can vary from economy to economy, depending on the specific needs, culture, and status of a nation's technological development. It is important to bear in mind that the process of building a strategic framework includes setting continuous and comprehensive communication among the stakeholders involved, and providing for inclusive, transparent and responsive cooperation amongst public and private sectors, academia, and civil society.

The overall goals of the national cybersecurity strategies identified by all WB economies aim to enhance information security of governmental bodies, secure stable operations and resilience of ICT systems of special importance (essential services), improve the protection of critical information infrastructure, raise awareness and improve knowledge on information security among citizens and entrepreneurs, increase capacities for the fight against high-tech crime, provide a safe environment for the private sector and digital businesses, and create a platform for cooperation between the public and private sector and participation in regional and international initiatives. All regional NCSs envision further development of the legislative framework by forming multi-sectoral national cybersecurity coordination bodies or councils, tasking relevant institutions in the field of cybersecurity to establish CIRTs, or identify staff members whose basic tasks will be related to the activities from the cybersecurity domain.

Action plans for implementing of NCSs with defined time frames, budget allocation, roles and responsibilities as well as preferred indicators are mostly in place in all WB economies, yet the effective implementation, monitoring and evaluating of these mechanisms remains the challenge. Western Balkan economies still need to invest efforts in creating a sustainable system of policymaking among the key institutions in charge of developing and adopting a strategic environment for cybersecurity that will be able to review, assess, adapt and revise national cybersecurity priorities systematically.

The following regional review will offer valuable insights on the national cybersecurity strategy of each WB economy, explaining governance and institutional structures, regulatory frameworks, specific priority areas of each economy, risk assessments and management procedures, capacity building and awareness raising programs, as well as regional and international cooperation approaches. The review follows the structure of the Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity (2018)[1] and examines if and how the national strategies follow the good practices recommended in the Guide.

[1] http://handle.itu.int/11.1002/pub/811cf62d-en . The Reference Guide was drafted in a democratic process among partnering organizations gathered by the International Telecommunications Union (ITU).

II Overview of national cybersecurity strategy frameworks of Western Balkan economies

ALBANIA

Competent institution: National Cybersecurity Agency - national CIRT of Albania previously known as ALCIRT, now imbedded as part of the National Authority for Electronic Certification and Cybersecurity (AKCESK)

Three main authorities in Albania are responsible for addressing different categories of incident response. The Ministry of Defence (MoD) is responsible for handling the MoD and Air Force related cyber-incidents. The Albanian State Police and the office of the prosecutor's Cybercrime Investigation Unit handle cybercrime incidents. However, AKCESK serves as the official national coordinating body for the reporting and management of cybersecurity incidents for important information infrastructures and critical information infrastructures operators[2].

Legislation and strategic framework in place:

The Council of Europe Convention on Cybercrime (Budapest Convention), ratified by Albania on 25.04.2002 via Law No. 8888

Law No. 9918, dated 19.05.2008, "On Electronic Communications in the Republic of Albania", as amended

Law No. 9887, dated 10.03.2008, "On protection of personal data", as amended

Law No. 2/2017 "On Cybersecurity" (2017)

National Cross-cutting Strategy "Digital Agenda of Albania 2015-2020"

Regulation on the content and method of documenting security measures (2018)

Decision of Council of Ministers No. 141, dated 22.03.2017, on "Organizing and functioning of the National Authority for Electronic Certification and Cybersecurity" (2017)

Decision on approval of the list of critical information infrastructures and list of important information infrastructures (2018)

Methodology for identification and classification of Critical Infrastructures and Important Information Infrastructures

Policy paper on Cybersecurity 2015-2017 (2015)[3]

Other relevant legislation, as listed in the Policy paper:

Criminal Code (2008)

[2] Global Cybersecurity Capacity Centre (2019), Cybersecurity Capacity Review of Albania, p8. Available on: https://cesk.gov.al/publicAnglisht_html/Publikime/2019/AlbaniaCMMReport.pdf

[3] In addition to the Law on Cybersecurity, the policy paper presents the only strategic document currently in place in the Republic of Albania. For this reason, strategic priorities are, for the purpose of this report, drawn from this document.

National CERT/CSIRT/CIRT: AKCESK, the National Authority for Electronic Certification and Cybersecurity

OVERARCHING PRINCIPLES

Vision: Working towards a safer, more reliable and more sustainable cyberspace for citizens, business and government in support of economic and social development in Albania.

Seven principles are defined, namely:

- Protection of fundamental human rights, freedom of speech, personal data and privacy
- Provision of access for all citizens
- Shared responsibility
- Strengthening cooperation and coordination
- International cooperation
- Administration of risk
- Abiding by the values defined in the policy paper

Comprehensive approach and tailored priorities: Seven strategic objectives are defined by the policy paper:

- Complete the legal framework on cybersecurity
- Raise awareness of cybersecurity
- Increase the levels of knowledge, skills and capacities for expertise in cybersecurity
- Identification and protection of Critical Information Infrastructure (CIIP)
- Develop and implement minimum cybersecurity requirements
- Increase investments in order to enhance security in state networks/systems
- Strengthen partnerships with other counterpart structures inside and outside the country

Inclusiveness: The policy paper states that in the process of drafting the document, all stakeholders from the public and private sector have been consulted with, and that assistance has been provided by the European Union through TAIEX.

Economic and social prosperity: N/A

Fundamental human rights: The policy paper lists protection of fundamental human rights, freedom of speech, personal data and privacy as one of its basic principles. It explicitly states that cybersecurity can be efficient only if based on fundamental rights and freedoms pursuant to the Charter of Fundamental Rights of the European Union and universal values of the EU. Reciprocally, the rights of individuals cannot be ensured without having safe networks and systems in place. To this end, the paper states that every exchange of information, when it includes personal data, should be made in accordance with the EU legislation on personal data protection.

In addition, providing safe access to citizens, as well as ensuring both the integrity of the internet and an unlimited information flow also constitutes one of the paper's basic principles.

Risk management and resilience. The policy paper states that necessary measures for the administration of risk will be taken, based on best standards and practices, in order to ensure cybersecurity.

Appropriate set of policy instruments: Other than the policy paper on Cybersecurity, a Law on Cybersecurity was also adopted in 2017. Furthermore, a methodology for identification of critical infrastructure has been developed and a list of identified critical infrastructures adopted. The content and method of documenting security measures is also provided in the form of Regulation. The policy paper further envisions defining the legal/regulatory basis on which operators of critical infrastructures can report serious cyber-incidents. A national cybersecurity strategy (2018-2023) has been articulated and is under development.

Clear leadership, roles and resource allocation. The policy paper provides a list of government structures relevant for cybersecurity and crime. The central authority that identifies, foresees and takes measures against cyber threats/attacks in accordance with the legislation in place is the National Cybersecurity Agency (The national Computer Incident Response Team for Albania – previously known as ALCIRT, now part of AKCESK).

Other relevant institutions include:

- Classified Information Security Directorate
- National Authority for Electronic Certification
- National Agency on Information Society
- Albanian State Police
- General Prosecution Office
- State Intelligence Service
- Ministry of Defence
- General Staff of the Armed Forces
- Directorate for Encryption
- Intelligence Protection and Security Agency
- Bank of Albania
- Electronic and Postal Communications Authority
- Information Right and Personal Data Protection Commission

Additional institutions expected to support the achievement of stated objectives in the document include the Albanian School of Public Administration and the Education Development Institute.

GOOD PRACTICE

- Governance. The National Cybersecurity Agency is currently the lead institution on cybersecurity in the country. The 2017 policy paper states that Government institutions are to play a key role in terms of completing the legal framework in the field of cybersecurity; critical information infrastructure identification and protection; development and implementation of basic cybersecurity requirements; increasing investments; strengthening partnerships; raising awareness; and raising the level of knowledge, skills and capacity for expertise in this field. According to the Paper, Government institutions are also to develop the preconditions and encourage the private sector, non-governmental organizations and especially operators of critical infrastructures to take part in the processes of legislative framework development; identification of critical infrastructure; defining minimum requirements for cybersecurity; public-private partnerships and the like.

- The policy paper is to be monitored by an Interinstitutional Working Group assembled by the Prime Minister, the Minister in charge of Public Administration and Innovation, the National Cybersecurity Agency and the Department of Developing Programming, Financing and Foreign Aid at the Council of Ministers.
- Risk management in national security. The policy paper envisions development of standards, guidelines and procedures based on best international practice to be implemented in the public administration. Development and approval of risk analysis procedures concerning security for the systems used and electronic services provided by institutions is considered a priority.
- Furthermore, setting up business continuity centres and disaster recovery centres is to be encouraged, as well as a \monitoring system for institution networks.
- Preparedness and resilience. With acknowledgement that a significant number of critical infrastructures are in private hands, the policy paper highlights the need for ensuring continuity of business activities in cases of force majeure or various cyber-attacks. To this end, the Paper recognizes the need for encouraging operators of critical infrastructure to implement full security architecture (including risk management and emergencies) to ensure effectivity, reliability and continuity of the services provided.
- Critical infrastructure services and essential services. The policy paper refers to the concept of shared responsibility, stating that the challenge of cybersecurity affects all areas of life and society, necessitating security measures to be implemented by all users of ICT and cyberspace. This includes public institutions, the private sector and citizens. In order to abide by this basic principle, another principle - that of strengthening cooperation and coordination among the public and private sector and the academic world - is also defined. The need for clearly defining structures and procedures that will ensure coordination at the political-strategic and operational level by involving all actors in the public and private sector is also highlighted.
- In terms of critical infrastructure specifically, the Paper envisioned development of necessary procedures and processes for the identification of critical information infrastructure, as well as development and implementation of mandatory minimum-security procedures and standards. Development of minimum procedures is also envisioned.
- Capability/Capacity building and awareness raising. The policy paper clearly recognizes the need for raising awareness for cybersecurity. To this end, it envisions the Government undertaking initiatives to develop programmes of education and training of ICT users, covering all levels of public administration (e.g. IT experts, administrators of systems and ICT, and the like). Dissemination of information on the risks and issuance of instructions and advice for minimum security of ordinary users is

envisioned as an ongoing process. Close cooperation with the media is also defined as the fastest way of spreading necessary information as widely as possible.

- An assessment on the introduction of educational programmes in pre-university levels is also listed as an intended activity by the policy paper.
- Finally, cooperation with the private sector, namely, electronic communication companies, internet service providers, the banking and energy sector(s) is also mentioned, in order to raise awareness and encourage implementation of standards from the private sector.
- In terms of capacity development, the Paper lists activities pertaining to the introduction of cybersecurity in elementary schools, high schools and institutions of higher education. Institutional capacity development through tailored training as well as participation in NATO's Smart Defence Multinational Cyber Defence Education and Training Project is also envisioned.
- Legislation and regulation. In addition to the Law on Cybersecurity and a number of regulations pertaining to critical infrastructure identification and procedures for recording incidents, a cybersecurity strategy is currently being developed. The policy paper envisions development of a unified reporting system for individuals and businesses to report cybercrimes in order for necessary measures to be taken, and the institutions in charge of strengthening the law could define the level of impact of cybercrime on individuals and the economy in Albania. Cybercrime legislation per se is not mentioned in the Paper. Albania has ratified the EU Convention on Cyber-crime in 2002, which is reflected in the country's Criminal Code.
- International cooperation. International cooperation and coordination is defined as one of the basic principles of the policy paper. Albania's membership in NATO and aspirations of EU membership are recognized as key drivers for actively taking part in different initiatives and programmes in cybersecurity, in order to fulfil commitments to ally countries.

BOSNIA AND HERZEGOVINA

Competent institution(s):

Ministry of Communications and Transport of Bosnia and Herzegovina; Ministry of Security in Bosnia and Herzegovina

At entity-level: Federal Ministry of Transport and Communications at Federal level; and

Ministry for Scientific-Technological Development, Higher Education and Information Society of Republika Srpska.

Legislation and strategic framework in place:

Laws on Information/Cybersecurity do not exist per se; rather there exists a patchwork of legislation containing elements that relate to the field, both in Bosnia and Herzegovina, as well as at entity-level and in Brčko District.

Other relevant legislation, as mapped in the ITU Readiness Assessment Report[4]:

Law on Communications (2006)

Law on Electronic Signature (2006)

Law on Electronic Business Transactions (2007)

Law on Prevention of Money Laundering and Financing of Terrorism (2014)

Decision of Council of Ministers of Bosnia and Herzegovina on special obligations of legal and physical entities providing telecommunication services, administrating telecommunication networks and offering telecommunication services in relation to securing and maintaining capacities that shall enable the authorized agencies to carry out legal interception of telecommunications as well as capacities for safeguarding and ensuring telecommunications (2006)

National CERT/CSIRT/CIRT: Currently there is no overarching CERT/CSIRT/CIRT in Bosnia and Herzegovina.

Specific developments, taking place at entity level are listed below:

Entity level:	
Federation of Bosnia and Herzegovina	**Republika Srpska**
Competent institution: Federal Ministry of Transport and Communications	**Competent institution:** Ministry for Scientific-Technological Development, Higher Education and Information Society of Republika Srpska

[4] Readiness Assessment Report to Establish a CIRT Network in Bosnia and Herzegovina. August 2018. ITU.

Legislation and strategic framework in place:	**Legislation and strategic framework in place:**
Information Security Management Policy in the Institutions of the Federation of Bosnia and Herzegovina for the period 2018-2022 (2019) A Working Group has been assembled to produce draft legislation in the field of information/ cybersecurity.	Law on Information Security (2011) Regulation on Information Security Measures (2012) Rulebook on Information Security Standards (2012) A Cybersecurity Strategy is currently under development Other relevant legislation: Law on Electronic Signature (2008) Law on Electronic Document (2008) Law on Electronic Management (2009)
Competent CERT/CSIRT/CIRT: A Working Group has been assembled to foster development of a Federal CERT, hosted by the Federal Ministry of Transport and Communications	**Competent CERT/CSIRT/CIRT:** CERT-RS, hosted by the Ministry for Scientific-Technological Development, Higher Education and Information Society of Republika Srpska

An overarching cybersecurity framework in Bosnia and Herzegovina is still under development. Despite a lack of an overarching legal framework, there is a patchwork of legislative documents that touches upon this field. In addition, some sectoral policies have also been developed in the meantime, such as the Cybersecurity Strategy of the Ministry of Defence (2017) which focused solely on the MoD systems and is complemented by an action plan for its implementation.

Regarding strategic approaches, a strategy for the establishment of BiH CERT was proposed by the Ministry of Security of BH in 2011 and adopted. A working group was established the same year, producing an action plan for the establishment of BiH CERT. The action plan proposed the creation of a coordinating body by the Council of Ministers in order to mitigate potential challenges to establishing the BiH CERT and other CERTs in BH. The document was accompanied by a proposal of a final report on the work of the working group and was to be submitted to the Council of Ministers of BH in 2012. They were however, never officially adopted.

In 2015 the Council of Ministers of Bosnia and Herzegovina adopted a conclusion requesting the Ministry of Security of BH to draft a Decision on determining a BIH CERT, focused on the institutions of Bosnia and Herzegovina. Finally, in 2017, the Council of Ministers of Bosnia and Herzegovina adopted a decision on establishing a CERT team of Bosnia and Herzegovina, to be hosted by the Ministry of Security of BH.

A decision on the adoption of an Information Security Management Policy in the Institutions of Bosnia and Herzegovina for the period 2017-2022 was passed in the meantime, in March 2017. The Ministry of Communications and Transport of Bosnia and Herzegovina and the Ministry of Security of Bosnia and Herzegovina have been tasked to monitor implementation of this decision and report to the Council of Ministers.

At the entity level, the only official CERT in Bosnia and Herzegovina, for the time being, is CERT RS in Republika Srpska. The entity is also currently working on developing a cybersecurity strategy, through an interdepartmental working group appointed in 2016. Steps are also being made towards establishing a Federation CERT.

When it comes to matters such as cybercrime, there have been more developments. The EU Convention on Cyber-crime was ratified in 2006. However, legislative documents currently in force do not fully endorse it, making transposition of the document only partial. Therefore, matters pertaining to cybersecurity and cybercrime are dispersed across the penal codes and laws on criminal procedure of Bosnia and Herzegovina as a whole, as well as at entity level (Federal and Republika Srpska), including also the Brcko District. Existing legislation also does not cover all the issues the convention deals with, as for example, the human rights dimension is still missing.

KOSOVO[5]*

Competent institution: Ministry of Interior (MIA)

Legislation and strategic framework in place:

Law on Information/Cybersecurity does not exist per se; rather a patchwork of legislation exists containing elements that relate to the field. A list of laws and regulations relevant for this field is provided within the strategy.

National Cybersecurity Strategy and Action Plan 2016-2019 (2015)

Law on Critical Infrastructure (2018)

Other relevant legislation, as listed in the strategy:

- Constitution of the Republic of Kosovo
- Law on the Establishment of the Kosovo Security Council
- Law on Prevention and Fight Against Cyber-crime
- Law on the Information Society Services
- Law on Electronic Communications
- Law on Interception of Electronic Communications
- Law on the Protection of Personal Data
- Law on Police
- Law on Public Peace and Order
- Law on the Kosovo Intelligence Agency
- Law on the Execution of Penal Sanctions
- Law on Copyright and Related Rights
- Law on the Implementation of International Sanctions
- Law on International Legal Cooperation in Criminal Matters
- Law on International Agreements
- Law on Controlling and Supervising State Borders
- Law on Banks, Micro-Finance Institutions and Non-Bank Financial Institutions
- Law on the Kosovo Agency on Forensics
- Law on the Trade of Strategic Goods
- Law on Private Security Services
- Law on the Kosovo Security Force
- Law on Classification of Information and Security Clearance

[5] * This designation is without prejudice to positions on status and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

- Code on Customs and Excise Code of Kosovo
- Law on Amending and Supplementing Customs and Excise Code in Kosovo

National CERT/CSIRT/CIRT: KOS-CERT, hosted by the Regulatory Authority of Electronic and Postal Communications (RAEPC)

OVERARCHING PRINCIPLES

Vision: Ensure a safe cyberspace environment by minimizing and preventing cyber-threats in cooperation with national and international partners.

The strategy states that the document itself was designed based on assessments and analysis of law enforcement agencies, government and local and international organizations, global trends, and practices and policies of the European Union. It was developed by applying comparative methods in terms of best practice, alongside using theoretical literature and empirical studies. It defines nine key principles:

- Constitutionality and Legality
- National Security
- Subsidiarity
- Holistic Approach
- Public and Private Partnership
- Continuity
- Confidentiality
- Human Rights and Freedoms
- International Cooperation

Comprehensive approach and tailored priorities. The five strategic objectives defined by the strategy are:

- Critical information infrastructure protection
- Institutional development and capacity development
- Building public and private partnerships
- Incident response
- International cooperation

Inclusiveness: The strategy states that the document was drafted by a working group formed by the Ministry of Interior and included all state institutions, professional associations, private sector, civil society and international partners. Involvement of representatives of financial institutions is explicitly highlighted.

Economic and social prosperity: N/A

Fundamental human rights: Observance of basic rights and liberties are explicitly referred to in the document, with the protection of privacy and property of network users to be primarily ensured by increased cybersecurity. Balancing security and privacy is seen through the lens of adopting necessary measures to protect and guarantee national cybersecurity, while respecting privacy, fundamental rights and liberties, free access to information as well as other democratic principles.

Risk management and resilience: N/A

Appropriate set of policy instruments: The strategy recognizes that there is no umbrella cybersecurity legislation but lists a set of primary legislative documents that cover various aspects related to the field, including regulations and criminal codes. A reference to aspects of compliance with the Cybersecurity Strategy for the European Union, ENISA Guidebook on National Cybersecurity Strategies as well as cybersecurity strategies of EU Member States is also made.

Clear leadership, roles and resource allocation: The Minister of Internal Affairs is the National Cybersecurity Coordinator, responsible and mandated to coordinate, guide, monitor and report on the implementation of policies, activities and actions related to the strategy, while the Ministry of Internal Affairs has a functional role in achieving the objectives set by the document.

Other public bodies for which the strategy states specific roles in the national institutional mechanism include:

- Kosovo Judicial Council
- Kosovo Prosecutorial Council
- Prosecution and Courts
- Secretariat of the Kosovo Security Council
- Kosovo Intelligence Agency
- Ministry of Justice
- Ministry for the Kosovo Security Force
- Ministry of Economic Development
- Ministry of Finance
- Ministry of Education, Science and Technology
- Ministry of Foreign Affairs
- Ministry of European Integration
- Regulatory Authority of Electronic and Postal Communications
- Agency for Information Society
- National Agency for Protection of Personal Data

In terms of resource allocation, this can be inferred from the action lan for implementation of the strategy. The action plan lists activities, time frames, budget sources, responsible and supporting institutions as well as preferred indicators. A very limited number of activities however have a precise indication of the resources necessary for implementation. These include implementation of the system for cyber threat prevention in Kosovo Police and governmental institutions; advancement of equipment for Kosovo Police to investigate cybercrime; and advancement of the technology in the Kosovo Forensics Agency. All other activities state that they are either a budgeted or administrative cost or a donation. A number of partners for implementing activities are listed alongside lead competent institutions for each of the activities, including the OSCE and UNDP, as well as the ICITAP and ENCYSEC programmes and project respectively.

Trust environment. There are no explicit mentions of building trust among stakeholders. Public-private cooperation is mainly referred to in terms of ensuring engagement of relevant critical infrastructure (which is in private hands), as well as advise from experts from the private sector regarding development of cybersecurity curricula.

GOOD PRACTICE

- Governance: There is acknowledgement that multi-stakeholder approaches are key for cybersecurity and that, for this reason, coordination of the competent and relevant governmental authorities is necessary. Accordingly, this can only be done by an entity in a position to perform such a task considering the various actors involved. The strategy sets out for a National Cybersecurity Council to be established to strengthen cross-sector, public-private cooperation, inclusive of representatives of the following institutions: Ministry of Internal Affairs; Kosovo Police; Kosovo Forensics Agency; Ministry of Kosovo Security Forces; Kosovo Intelligence Agency; Agency for Information Society; Kosovo Security Council; Ministry of Justice; Kosovo Prosecutorial Council; Kosovo Judicial Council; Ministry of Finance; Kosovo Customs, Ministry of Education; Science and Technology; Ministry of Foreign Affairs; Regulatory Authority of Electronic and Postal Communications; Central Bank of Kosovo. Business representatives are to be invited as associate members, while representatives of academia would be involved on a technical level.
- Risk management in national security: Ensuring full functionality of CERTs/CSIRTs is an integral and vital part of the strategy, as it acknowledges that policies should be in place covering practical steps and organization needs to take when an incident occurs.
- Preparedness and resilience: N/A
- Critical infrastructure services and essential services.: The strategy envisions identification of critical information infrastructures following these steps: determination of services that could be classed as critical; identification of infrastructures that are technically indispensable for running these services, introduction of objective criteria for the level of protection each identified infrastructure element needs, and checking the identified criteria through conducting regular cyber exercises.
- Public/private partnerships are also recognized as a necessary concept and envisioned through the definition of procedures on information exchanges with internet service providers (ISPs), the banking sector, electric power providers, water supply companies, transport companies (air and ground), as well as academia. Joint activities are to focus also on education on cybersecurity, in terms of providing advice on cybersecurity curriculum in relation to certification of information security experts and further development of learning modules.
- Capability and capacity building, and awareness raising: A culture of cybersecurity is to be promoted across society through partnerships with the education system and industry and through targeted events. Measures to be taken include management of expertise and knowledge through tailored training, participation in national and international exercises, and awareness tools and information campaigns for citizens. There is special recognition of the need for executive level staff in organizations to have sufficient understanding of the cyber domain. Consequently, cyber aspects are to be integrated into the existing curricula.

- In terms of human capacity building, development of training curricula is envisioned, organizing tailored training for different groups alongside engaging in cyber exercises at national and international level.
- Research and development is recognized as a key component for improving responses to cybersecurity threats. Development of R&D capabilities is thus envisioned, to be used also for engaging in national and international projects according to resources available.
- Legislation and regulation. With the main goals of harmonizing the legal framework with the European Union, two pieces of legislation are envisioned by the strategy:
    - Law on Identification and Protection of Critical Infrastructure, an important part of which will be dedicated to Critical Information Infrastructure Protection (CIIP)
    - Law on Preventing and Combating Cybercrime with appropriate bylaws covering cybersecurity
- International cooperation. International cooperation is to be practiced through bilateral or multilateral agreements with key allies and other like-minded nations to strengthen cooperation on cybersecurity, regional forums with a focus on capacity building initiatives within the Western Balkans region, and cooperation with international organizations helping promote best practice and fostering a coordinated global approach to combating cybersecurity threats.
- Membership in Trusted Introducer and FIRST communities is also explicitly listed within the activities allowing functionalisation of a national CERT/CSIRT and other CERTs/CSIRTs. Out of the two, the national CERT, KOS-CERT is an accredited member[6] of Trusted Introducer.

LIFE CYCLE

The strategy explicitly lists the phases of the document's life cycle, aimed at ensuring continued progress on the document itself, as well as procedures and products, in accordance with any changes that took place in the immediate and wider environment. Relying on the life cycle phases defined by ENISA; these refer to:

- Development
- Implementation
- Evaluation
- Adaptation of the strategy

and involves periodical reviews of the strategy, updating both this document as well the action plan(s).

[6] Accredited since 3 July 2017.

MONTENEGRO

Competent institution: Ministry of Public Administration and National Security Agency of the Ministry of Defence (as of November 2020)

Legislation and strategic framework in place:

- Law on Information Security (2010)
- Law on Amendments to the Law on Information Security (2016)
- Law on classified information (2020)
- Regulation on Information Security Measures (2010)
- Regulation on amendments to the Regulation on Information Security Measures (2015)
- Cybersecurity Strategy 2013-2017 (2013)
- Cybersecurity Strategy 2018-2021 (2017)7
- Action Plan for the implementation of the Cybersecurity Strategy 2018-2021 for 2019 (2019)8
- Methodology for the Identification of Critical Information Infrastructure (CII) and Action Plan (2014)
- Rules of Procedure for CIRT.ME (2017)

Other relevant legislation, as listed in the Cybersecurity Strategy 2013-2017 (2013):

- Criminal Code
- Criminal Procedure Code
- Law on the National Security Agency
- Law on Classified Information
- Electronic Signatures Law
- Law on Electronic Communications
- Electronic Commerce Law

National CERT/CSIRT/CIRT: CIRT.ME, hosted by the National Security Agency of the Ministry of Defence

OVERARCHING PRINCIPLES

Vision: The strategy does not provide a single, clearly defined overall vision. It does however refer to the EU NIS Directive, with Montenegro being an aspiring member state, and the NATO Defence Pledge, as a member of the alliance. The strategy states that the government will continue to undertake activities directed towards implementing the strategy for identification of strategic goals, ensuring further advancement of the concept of

[7] Montenegro is the only economy out of the WB6 that is already on its second National Cybersecurity Strategy. The previous one covered the period 2013-2017.

[8] Action plan for implementation adopted year to year.

cybersecurity in Montenegro compatible with the concepts of the most developed member states of EU and NATO. Special attention will be dedicated to alignment in terms of standardising terminology, methods, policies and procedures with adopted European and international standards. Eight key principles are defined:

- Cyber defence capacities
- Centralization of cyber expertise and resources
- Protection of critical information infrastructure
- Cross-institutional cooperation
- Data protection
- Cybersecurity education
- Public-private partnership
- Regional and international cooperation
- Comprehensive approach and tailored priorities: Based on the eight strategic principles stated above, the strategy defines the following strategic goals:
- Further strengthening of the cybersecurity capacities in the sense of providing adequate human and financial resources as well as meeting other needs necessary for efficient and agile cyber capacities of Montenegro institutions aimed at ensuring safe cyberspace, providing business incentives and ultimately contributing to the economic prosperity of Montenegro.
- Undertake activities with a view to centralizing and gathering expertise in the field of cybersecurity in order to: strengthen capacities for the purpose of responding efficiently to sophisticated cyber threats against critical information structures and other important information systems; understand risks to cyberspace of Montenegro; provide adequate recommendations and improve cooperation with the private and public sectors.
- Continue to strengthen the CII defence capabilities, and since the National CIRT has a key role in this field, it must have adequate resources and tools to effectively understand, analyse and respond to the wide spectrum of threats in this field.
- The need for strengthening inter-institutional cooperation has been identified, whereby a special accent will be placed on efficient and timely exchange of information and best practices. In this context, the responsible institutions will work on strengthening communication methods through, among other things, organization of exercises for crisis communication in the case of cyber-incidents and large-scale attacks. The exercises will be aimed at defining clear communication procedures in crisis situations as well as their timely revision.
- Strengthen the national capacities necessary for security accreditation of communication and information systems and the processes where classified information is used, as well as the capacities in the field of crypto protection;
- In order to achieve the best cybersecurity practice, the responsible bodies will learn about the newest cyber threats and undertake activities on educating citizens and organizations about protection mechanisms in cyberspace. Sustainable, continuous and coordinated efforts are necessary to achieve wider changes in behaviour and secure that all target groups, public and private sectors, as well as individual citizens, understand risks and threats in cyberspace.

- Continue with dedicated work aimed at supporting the response to incidents and sharing of information and joint initiatives in partnership with private sector. Therefore, a high level of communication, cooperation and integration is the most efficient way to understand and properly respond to the needs and challenges of private companies with the aim of undertaking the necessary measures and achieving a sufficient degree of security.
- Continue with regional and international activities and exercise its influence by investing in partnerships which shape global evolution of cyberspace in the manner which improves and spreads economic and security interests and strengthens collective security.

Inclusiveness: There is no specific mention of the actors involved in the process of strategy development.

Economic and social prosperity: The strategy highlights that the Government of Montenegro is devoted to growth and prosperity through strong cybersecurity, as safe cyberspace provides business incentives ultimately contributing to the economic prosperity of the country.

Fundamental human rights: No mention of human rights in the strategy.

Risk management and resilience: The strategy sets out that relevant institutions must have capacities to recognize, identify and conduct annual risk analysis, or if necessary, risk analysis for a shorter period of time, which will be related to information systems within their own institutions or within their scope of work.

Appropriate set of policy instruments: In addition to the Law on Information Security and two iterations of the national cybersecurity strategy, a methodology for the identification of Critical Information Infrastructure (CII) and a complementary action plan are in place. Based on this methodology, the Ministry of Public Administration defined a list of critical infrastructures in the country.

Adoption of secondary legislation for protecting CII is envisioned by the strategy. This regulation should define the procedures for communication between owners of CII and responsible institutions, as well as basic technical and organizational measures that owners of CII must implement.

In addition, amendments to existing regulation for implementing certification of communication and information systems and processes where classified data is involved is also planned.

Drafting of procedures for exchange of information on cyber-incidents, the ways of communicating in the case of cyberattacks, and the ways of assistance and cooperation between public and private sectors is also envisioned by the strategy.

The strategy makes repeated reference to the EU NIS Directive, ENISA documents and guides and the NATO Cyber Defence Pledge as guiding documents for developing the strategic and operational framework.

Clear leadership, roles and resource allocation: The competent institution for cybersecurity is, as of November 2020, the National Security Agency of the Ministry of Defence, which also hosts the national CIRT (CIRT.ME). With the adoption of amendments to the existing law on classified information in 2020, the CIRT.ME is placed within the MoD with competence for coordination, prevention and protection of information systems of both state and non-state actors. This changes still needs to be reflected in other sectoral regulation and strategies. The new Law on Information Security will be adopted in the course of 2021. Back in 2017, a Cybersecurity Council was formed, comprising of representatives of the Ministry of Public Administration, Ministry of Defence, Ministry of Interior, Ministry of Justice, National Security Agency and the National Security Authority.

Institutions defined as being accountable for cybersecurity in Montenegro are: National Security Agency of the MoD within which the national CIRT operates; Ministry of Public Administration; Ministry of Interior/Police administration; Ministry of Justice; Ministry of Education; and Directorate for Protection of Confidential Data.

The strategy highlights that budgetary funds must be allocated every year to separate bodies or organizational units within institutions that have been identified as key for Montenegro's cybersecurity system so that they can procure adequate resources and tools for the effective functioning.

In terms of resource allocation, this can be inferred from the action plan for implementation of the strategy. The action plan lists indicators of success compared against the initial situation, expected developments during the process of implementation and end result. These are further broken down into specific activities, result indicators, lead institutions, timeframes for implementation, envisioned resources, and sources of funding. Exact amounts are expressed only for two activities: establishment of a security operations centre (SOC), and development of a platform for information exchange at the Ministry of Public Administration, both of which are expected to be funded from the budget. For all other activities, the action plan generally states that no specific resources are required and only one activity - strengthening cross-institutional cooperation - is to be funded through donations.

Trust environment: Trust is mentioned within the strategic objective of building partnerships between the public and private sector. According to the strategy, establishing of efficient cooperation among stakeholders is one of the main challenges precisely due to different interests, trust, competition and lack of clear managerial structure. Trust is defined as a process that requires extensive dialogue, time and effort. In addition, trust of citizens in institutions and companies doing business online is also highlighted as a challenge by the document, caused by inadequate communication and cooperation between the public and private sector.

GOOD PRACTICE

- Governance: The competent ministry for cybersecurity is the Ministry of Defence, which reports to the Information Security Council on matters pertaining to this topic. Other relevant ministries and public bodies mentioned include the Ministry of Interior, Ministry of Justice, Ministry of Education, Ministry of Foreign Affairs, National Security Agency, Army of Montenegro, Police Administration, and Directorate for Protection of Confidential Data.

- In terms of cross-institutional cooperation, the strategy envisions appointing contact persons for cybersecurity on behalf of all actors involved in order to further facilitate cooperation and communication among institutions.

- Risk management in national security: Although the strategy contains no specific reference to incident classification, the rules of procedure for CIRT.ME (which are publicly available) offer a categorization of different incidents divided by incident category, incident type and examples. These categories are then assigned different levels of priority.

- Preparedness and resilience: The strategy envisions that relevant institutions in the field of cybersecurity will establish CIRTs or identify staff members whose basic tasks will be related to the activities from the cybersecurity domain: so-called local CIRTs.
- Specific measures for development of the national CIRT are outlined in the strategy. These include an increase in the number of staff, as well as division into two different departments for incident response and for strategic goals and prevention. Adequate equipping of the national CIRT is also envisioned.
- Within the scope of cross-institutional cooperation, the strategy envisions establishment of a publicly available registry of cybersecurity experts which would be managed by the ministry responsible for this field, as well as development of a platform for dialogue and exchange of information which would connect cybersecurity experts from public and private sectors, both at local and national level.
- Critical infrastructure services and essential services: According to the strategy, owners of identified CII are required to conduct annual risk analysis.
- The national CIRT, in cooperation with other responsible CIRTs, is in charge of reviewing the analyses, and providing assistance in making analyses where CII owners do not have sufficient capacities. Additionally, the national CIRT, in cooperation with other CIRTs, should establish and formalize strategic partnerships with owners of CII, where, among other things, exchange of information should be specified, as well as the manners of exchanging information and expertise.
- The strategy further lists establishment of public-private partnerships as one of its key strategic objectives. To this end, institutionalization of cooperation among public and private sectors is envisioned.
- Capability and capacity building and awareness raising: The strategy envisions that the national CIRT will regularly organize specialist exercises, simulation of attacks against CII and large-scale attacks, for members of relevant bodies, as well as companies accountable for CII.
- Capacity building is specifically planned in the field of classified information. Namely, the strategy lists the following planned activities: (1) strengthening of information capacities of the state authority in charge of security accreditation of communication and information systems and processes where classified information is used (Security Accreditation Authority - SAA), and the state authority responsible for handling materials for cryptographic protection of secret data (National Distribution Authority - NDA) is also listed; and (2) Certification of communication and information systems where information marked with higher level of classification is used, the introduction of security information management system and risk management in communication and information systems where classified data marked as INTERNAL and unclassified sensitive information.
- In terms of long-term strategic directions, the strategy also envisions establishing cooperation with educational and scientific institutions with the aim of education and training of personnel, for the needs of creating national cryptographic solutions.
- When it comes to awareness raising, the strategy envisions participation in and organization of conferences, workshops, training, as well as with production of publications, drafting of papers and articles, and participation in educational programmes, and continuous improvement of materials published on the CIRT.ME por-

tal (tips, warnings, announcements, guidelines, rulebooks, presentations, webinars, lectures).

- Planned activities in the field of education focus on raising awareness on cybersecurity of teaching staff, mapping school pedagogues and psychologists as a specific target group that needs to be digitally literate first and trained on cybersecurity matters.
- Furthermore, in addition to regular subjects such as Informatics and Technique taught from the fifth grade of primary school, the strategy acknowledges the need for setting up extra-curricular activities for school children. Preparation of special materials for young children is also highlighted, to be distributed through school online portals.
- Legislation and regulation; In addition to the existing legislative framework, the strategy envisions adoption of secondary legislation for protecting CII, mainly focused on communication of these entities with responsible institutions, along with technical and organizational measures to be implemented.
- Drafting of a rulebook and procedures for exchange of information on cyber-incidents, the manner of communication in the event of cyberattacks, and the manner of assistance and cooperation among state authorities is also envisioned within efforts aimed at cross-institutional and public-private cooperation is envisioned by the document.
- When it comes to cybercrime, in order to strengthen the capacities of state law enforcement authorities, a High-Tech Crime Group has been set up at the Ministry of Interior to deal with instances of computer crime, child pornography, credit card and copyright abuse, placed within the section for fighting against organized crime and corruption. In addition, according to the strategy, the National Security Agency is also making significant efforts aimed at creating normative and operational mechanisms for fighting against cybercrime and espionage. Montenegro has ratified the EU Convention on Cybercrime in 2010.
- International cooperation. The strategy underlines continued cooperation within existing international communities, including ITU, NATO and FIRST, as well as efforts to establish new partnerships.

  CIRT.ME is a listed member[9] of Trusted Introducer, and a member of FIRST[10].

[9] Listed since 2 March 2013; re-listed on 14 March 2019.

[10] Member since 26 February 2013.

NORTH MACEDONIA

Competent institution: Ministry of Information Society and Administration

Legislation and strategic framework in place:

- Law on Information/Cybersecurity does not exist per se; rather a patchwork of legislation exists containing elements that relate to the field
- National Cybersecurity Strategy 2018-2022 (2018)
- National Cybersecurity Action Plan 2018-2022 (2018)

Other relevant legislation, as mapped in the Oxford CMM Report[11] (2018):

- Code of Civil Procedure (2010)
- Criminal Code (2013)
- Law on Personal Data Protection (2016)
- Law on Electronic Commerce (2014)
- Law on Electronic Communications (2013)
- Law on Criminal Procedure (2012)
- Law on Communications Monitoring (2012)
- Law on Interception of Communications (2012)
- Law on Electronic Management (2011)
- Law on Litigation (2010)
- Law on Electronic Data Form and Electronic Signature (2008)
- Law on Classified Information (2007)

National CERT/CSIRT/CIRT: MKD-CIRT, hosted by the Agency for Electronic Communications (AEK)

OVERARCHING PRINCIPLES

Vision: To have a safe, secure, reliable and resilient digital environment, supported by high-quality capacities, high-quality experts, built on trust, national and international cooperation in the field of cybersecurity.

Mission: To have clearly defined and sustainable policies, which will be coordinated in the manner of advancing national cybersecurity.

The key cybersecurity principles supporting the strategy are as follows:

- Effective and efficient cybersecurity capacities
- Protection and prevention
- Security for economic development
- Trust and availability

[11] 2018 Cybersecurity Capacity Review Former Yugoslav Republic of Macedonia. July 2018. GCSCC.

- Legal security

Comprehensive approach and tailored priorities: The five key goals defined by the strategy are:

- Building a cyber resilient ICT infrastructure, identifying and implementing adequate solutions in order to protect national interests;
- Promoting a cybersecurity culture in order to raise public awareness and understanding of cyber threats, as well as building and advancing the necessary capacities for protection;
- Strengthening national capacities for prevention, research and adequate response to cybercrime;
- Strengthening capacities for cyber defence of national interests and reducing current and potential cyberspace risks;
- Cooperation and exchange of information at the national and international level.

Inclusiveness: The strategy states that the document itself was prepared by representatives of three key ministries, namely, the Ministry of Information Society and Administration (5 representatives), Ministry of Interior (3 representatives), and Ministry of Defence (3 representatives). It also states that the first draft of the strategy has been amended into a mature draft version through implementation of comments and suggestions from “all stakeholders” before it was officially completed, although the stakeholders involved in this process are not explicitly listed.

In terms of stakeholders covered by the strategy, these include:

- Public sector, including authorities and other subjects representing both users of cyberspace and subjects that are obliged to apply the measures arising from the strategy;
- Private sector, referring to legal and business entities which are subject to special regulations including critical infrastructure and the security and defence systems; subjects who represent users of cyberspace as well as subjects that are obliged to apply the measures arising from the strategy;
- Academic community, in terms of educational institutions from the public and private sector, with a crucial role in developing a strong body of knowledge in the field of cybersecurity; and
- Citizens and civil society organizations, encompassing users of ICT and services, with special emphasis that citizens are not only to be seen as active users, but also to be considered as subjects who have their personal data present in cyberspace.

Economic and social prosperity: With the development of a digital economy, the strategy envisions the implementation of new ICT solutions and practices, as well as the global connectedness, as contributing to economic growth, minimizing at the same time negative externalities as a consequence of security incidents in cyberspace.

Fundamental human rights. The strategy clearly states that principles of basic human rights and liberties are to be adhered to in the process of implementing cybersecurity measures.

Among other, the following universal values are mentioned:

- Accessibility

- Freedom of expression
- Guaranteed information flow
- Information integrity
- Personal data protection
- Privacy
- Reliability
- Transparency

The universal application of international legal acts related to human rights, freedom of expression and privacy protection in explicitly underlined.

Risk management and resilience: Cyber-resilience is one of the five key stated goals of the strategy. The necessity of identifying all relevant capacities for cybersecurity across all relevant stakeholders, and to define specific jurisdiction and activities in function of improving cyber-safety and managing cyber-incidents is recognized. Activities for obtaining this goal include, among other: advancing the capacities and capabilities of MKD-CIRT; identification and protection of CII and IIS; developing national incident management procedures and protocols for times of peace, crises, state of emergency and state of war where every institution has a pre-defined role; developing a methodology for national-level cyber threat risk evaluation; establishing a single and comprehensive legal framework for cyber resilience; and defining precise procedures for safekeeping and protection of data processed by CII and IIS. Regular audits of CII and IIS, as well as continuous monitoring and evaluation of threats and risks, standards, and procedures, as well as CII and IIS operations and practices are also listed as envisioned activities.

Appropriate set of policy instruments: The strategy explains that the process of adoption of the document is predominantly related to, among other things, strengthening the cybersecurity institutional and legal frameworks, albeit without no explicit mention of adopting a stand-alone cybersecurity law as such, as well as defining and developing a cyber-defence policy. Explicit mentions referring to envisioned legislative frameworks pertain to the field(s) of cyber-resilience, cybercrime and cyber-defence.

The document also states that the strategy is based on the principles of the Cybersecurity Strategy of the European Union and the NATO Cyber Defence Pledge.

Clear leadership, roles and resource allocation: The strategy was developed by three ministries: Ministry of Information Society and Administration, Ministry of Interior, and Ministry of Defence. The Ministry of Information Society and Administration is in charge of further implementation of the strategic framework related to cybersecurity. In addition, legislative frameworks for cybercrime and cyber defence are envisioned by the strategy. Finally, the strategy envisions the establishment of an additional two bodies: a National Cybersecurity Council, to be established by the Government; as well as a Body with operational cybersecurity capacities either as a new entity, or as a separate organizational unit within an existing state entity.

In terms of resource allocation, this can be inferred from the action plan for implementation of the strategy. The action plan lists activities, the method of implementation, preconditions, priority levels, lead institutions and partners, financial sources and time frames. However, there are no indications of the exact resources needed for any of the envisioned activities. In addition, a significant number of activities is to be funded through donor support or various programmes of international organizations such as NATO.

Trust environment: Trust is mentioned in the strategy in the context of citizens' trust in digital services and electronic commerce. These are seen as directly contributing to the development of the digital economy and global recognition of North Macedonia as a safe environment for investment and business.

Additionally, the notion of trust is also highlighted as one of four key risks for proper implementation of the strategy, especially between the public and private sector, with the acknowledgment that development of trust requires dialogue, as well as extensive time and effort.

GOOD PRACTICE

- Governance: The strategy envisions further development of the legislative framework, namely in the field of cybercrime and cyber defence. Definition of procedures for cooperation and exchange of information across all stakeholders is also recognized as essential. As for cybersecurity, a specific law on cybersecurity does not exist per se; rather a patchwork of legislation exists containing elements that relate to the field.
- A list of stakeholders is also provided, mapping the public and private sector, the academic community and citizens and civil society organizations as four actor clusters. Relations between these are not elaborated.
- Furthermore, the strategy states that responsibility for implementing the measures defined within the document will be coordinated by the National Cybersecurity Council, while relevant authorities, ministries and other institutions are to analyse their current legislation and update regulations and procedures accordingly, delivering periodic implementation reports to the Council.
- The National Cybersecurity Council is to be established by the government, and responsible for monitoring and coordination of the strategy's implementation; suggesting measures for amending the strategy and action plan; participating, coordinating and aligning activities of the Security Council of North Macedonia; developing programmes and action plans for activities in the field of cybersecurity to be implemented by the body with operational cybersecurity capacities. The action plan for implementation of the strategy however states that the council is to be transformed from the National ICT Council into the National ICT and Security Council, which consists of ministers.
- The mentioned body with cybersecurity capacities is another entity envisioned by the strategy, to be established either as a separate, newly established entity (agency or directorate), or as a newly formed organizational unit within an existing state body. It is to be in charge of operationalizing the strategy and action plan and the directions set out by the National Cybersecurity Council, mainly pertaining to monitoring trends in cybersecurity; providing recommendations, opinions, research and reports related to the implementation of strategic documents in cybersecurity; organizing national and international exercises in the field; and the like. The action plan states that until this body is operational, these activities are to be conducted by the working group tasked to conduct activities stemming from the strategic documents in the field of cybersecurity.
- Risk management in national security: In terms of sectoral policies, development of cyber defence capabilities in the armed forces is seen as part of a comprehensive national defence approach. The need for full compliance with standards and directions provided by organizations such as the EU and NATO is defined as a prerequi-

site for participation in collective defence. To this end, development and implementation of common cybersecurity capacities, standards and training in cyber defence is seen as one of the key goals of the strategy. Activities enabling achievement of such goals include, among others: defining national cyber defence capacities (including military capacities of the Ministry of Defence and the armed forces); developing a single and comprehensive cyber defence legal framework; establishing a cyber defence system for national critical infrastructure; developing a system and programmes for exchange of information, knowledge and experience between the public, private and defence and security sector in the field of cyber defence; and establishing and sustaining international cooperation, joining efforts in combating shared cyber threats.

- Preparedness and resilience: Establishment of a single comprehensive legal framework for cyber resilience is among the five key goals defined by the strategy. As a concept, resilience is mainly referred to in the context of critical information infrastructure (CII) and important information systems (IIS).
- Critical infrastructure services and essential services: Within the principle of trust and availability, the strategy states that CII and IIS protection is of vital importance for North Macedonia. Alongside using state-of-the-art prevention, security and protection measures to mitigate incidents, the document also recognizes the need for developing well-prepared incident recovery plans with their effectiveness tested regularly through joint cyber exercises and simulations.
- Cooperation among all stakeholders with the capacity to contribute to cybersecurity - between the public, private and civil sector - is recognized as of the utmost importance. In order to improve such cooperation, the strategy envisions establishment of a Centre of Excellence. The Centre would facilitate exchanges of experience among the public and private sector (above all companies managing CII and IIS), civil society organizations and other institutions.
- Capability and capacity building and awareness raising: Within the principle of effective and efficient cybersecurity capacities, the strategy makes reference to supporting research and development, as well as education and training at all levels of society.
- One of the key goals of the strategy relates to cyber capacities and a cybersecurity culture. These are seen as the basis for inducing responsibility and understanding of cyber-related risks by all actors, developing a learned level of trust in e-services and users' understanding of how to protect personal information online, assuring a greater level of resilience across all levels of society. To this end, the strategy envisions exchanges of skills, knowledge and experience on a national level through ad-hoc inter-organizational research teams, comprised of experts in the public sector, private sector and the academic community.
- Specific activities for achieving the abovementioned goal include, among other, increasing cybersecurity capacities of SMEs, as well as the public and private sector in general, and CIIs; supporting research capacities and business innovations through the establishment of a scientific research centre in cybersecurity; adapting and refining existing study programmes in primary and secondary schools as well as developing study programmes and training in the area of cybersecurity at all levels. Developing adequate education and training programmes for public administration employees as well as managerial staff in the public and private sector (different levels) is recognized, as is the need for establishing retention mechanisms for ICT and cybersecurity staff.

- Legislation and regulation: Within the principle of protection and prevention, the strategy acknowledges that one of the main principles of the document is to support the national security system of the country.
- In terms of the overall national legislative framework, within the principle of legal assurance, the strategy states that the process of implementing cybersecurity measures, compliance with legal acts, principles of basic human rights and liberties, democracy and adherence to core values is essential.
- In terms of new legislative frameworks to be developed, the strategy mentions the field(s) of cyber resilience and cyber defence.
- The need for developing a specialized, detailed national plan for cybercrime management, including cyber-enabled crimes, is also explicitly recognized as one of the key goals of the document. To this end, the strategy envisions, among other, harmonization of the national legal framework with international policies related to cybercrime; developing a single, comprehensive legal framework and standards for fighting cybercrime; establishing formal procedures for cooperation and exchange of information in the field of cybercrime; advancing regional and international cooperation in this field; as well as continuous assessment of the adequacy and efficiency of such developed frameworks. North Macedonia has ratified the EU Convention on Cybercrime in 2004.
- International cooperation. One of the key goals of the strategy, cooperation and exchange of information, sees active international participation in tackling global challenges posed by cyber threats as an opportunity for increasing state capacities for handling cyber risks. To that end, alongside establishing and strengthening cooperation with other public and private CERT and CSIRT teams, academic communities, entities that manage CII and IIS and international organizations, the strategy also envisions, among other things, developing an effective cooperation model for all relevant institutions at the national level; developing mechanisms and procedures for international cooperation on a diplomatic level in case of cyber-incidents, attacks and crises; and promoting and advancing norms, rules and principles of responsible behaviour by the state according to internationally recognized principles.

  MKD-CIRT is an accredited member[12] of Trusted Introducer.

[12] Accredited since 8 December 2017.

SERBIA

Competent institution: Ministry of Trade, Tourism and Telecommunications

Legislation and strategic framework in place:

Law on Information Security (2016)

Law on Amendments to the Law on Information Security (2017)

Regulation determining the list of activities in the fields in which affairs of general interest are performed and in which information and communication systems of special importance are used (2016)

Regulation determining the measures for protection of information and communication systems of special importance (2016)

Regulation determining the content of the Security Act for information and communication systems of special importance, ways of verification and content of reports on security audits of information and communication systems of special importance (2016)

Regulation on the procedure for submitting data, lists, types and significance of incidents and the procedure of notification on incidents in information and communication systems of special importance (2016)

Regulation on the safety and protection of children in the use of information and communication technologies (2016)

Strategy for the Development of Information Security in the Republic of Serbia for the period 2017-2020 (2017)

Action Plan for the implementation of the Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020 (2018)

Strategy for the fight against high-tech crime for the period 2019-2023 (2018)

Other relevant legislation, as listed in the strategy:

Law on the Organization and Jurisdiction of Government Authorities in the Suppression of High-Tech Crimes (2009)

Penal Code (2016)

Law on Classified Information (2009)

Law on Personal Data Protection (2018)

Law on Electronic Communications (2014)

Law on the Military Security Agency and the Military Intelligence Agency (2013)

National CERT/CSIRT/CIRT: SRB CERT, hosted by the Regulatory Agency for Electronic Communications and Postal Services (RATEL)

OVERARCHING PRINCIPLES

Vision: The overall goal of the strategy is to develop and enhance information security in the Republic of Serbia and maintain it at an adequate level, in order to achieve stable operations of ICT systems of special importance (essential services); information security of citizens; increased capacities for the fight against high-tech crime; with the key underlying precondition for realising such goals being cooperation between the public and private sector, non-governmental organizations, the academic community and other actors.

Seven principles are defined, namely:

- Information security is an integral part of overall security and is in the function of exercising and respecting the rights, freedoms and interests of citizens, the economy and the state;
- Information security is important for all social factors using information and communication technologies, who need to be aware of the risks associated with the use of technology and to take preventive and other necessary protection measures;
- Information security means timely identification of risks, taking preventive measures and effective reaction to incidents;
- It is necessary to establish and improve the regular and efficient exchange of information on risks and incidents in the field of information security at the national and international level;
- Continue the continuous development of the system of protection in information security at the legal, organizational and technical level, with adaptability to new circumstances and challenges;
- Systematically raise awareness and improve knowledge and skills in all categories of citizens in terms of information security in everyday life and in the workplace;
- Establish continuous cooperation between the public and the private sector as a basis for the development and improvement of strategic priorities.

Comprehensive approach and tailored priorities: The Cybersecurity Strategy refers to the Strategy for the Development of an Information Society in the Republic of Serbia by 2020, sets the framework for the development of cybersecurity through five priority areas which are more concretely defined by goals that the Strategy aims to achieve:

- Security of information and communication systems, which refers to the risks of violating the functioning of the authorities, economy and organizations as a result of incidents in information and communication systems;
- Information security of citizens, which refers to the risks of violating citizens' safety by misuse of information and communication technologies;
- The fight against high-tech crime, which refers to the prevention and sanctioning of criminal offenses based on the abuse of information and communication technologies;
- Information security of the Republic of Serbia, which refers to the risks of violating national security through information and communication systems;
- International cooperation, which implies cooperation with foreign state bodies, international organizations and other partners in the field of information security.

Within the priority areas, the following strategic objectives are defined:

- In the field of information and communication security: (1) prevention and protection through information exchange, monitoring of current risks and awareness raising; (2) the security of ICT systems in business entities and the security of electronic business; (3) security of ICT systems of special importance; (4) security of classified information in ICT systems; and (5) cooperation between the public and private sectors in the field of information security;

- In the area of citizen security in the use of technology: (1) children's safety on the Internet; (2) protection of privacy and protection against abuse in the use of ICT; and (3) information security in the education system;
- In the field of combating high-tech crime: (1) improving mechanisms for detecting high-tech crime and prosecuting perpetrators; (2) raising awareness of the dangers of high-tech crime; and (3) the promotion of international cooperation in the fight against high-tech crime;
- In the field of information security of the Republic of Serbia: (1) an information security system of importance for national security; (2) development of scientific, technological and industrial capacities necessary for the protection of the information security of the Republic of Serbia; (3) building military capabilities of the defence system to defend against high-tech attacks; and (4) building security and intelligence capabilities in the field of information security;
- International cooperation.

Inclusiveness: Apart from relevant public institutions, the working group in charge of drafting the strategy also included representatives of international organizations, namely the OSCE Mission to Serbia and UNICEF, although this is not explicitly mentioned in the document.

Economic and social prosperity. The strategy recognizes that social and economic prosperity, national security and the defence of the Republic of Serbia directly and indirectly depend on ICT networks that extend within and outside the national borders in a complex, dynamic and often unpredictable environment.

Fundamental human rights: Although not referencing the aspect of human rights directly, the strategy dedicates a sub-chapter to the protection of privacy. To this end, the document acknowledges the need for further developing the legislative framework governing personal data protection, in line with EU standards, while at the same time removing possible obstacles for more efficient application laws in this field. Awareness raising on methods to protect personal data online and avoid excessive sharing of such information is recognized as a suitable activity to this end.

Risk management and resilience: The strategy recognizes the role of public-private cooperation in this field, stating that the academic community on the one side, and the private sector on the other, could showcase good practice examples in this field, highlighting the importance of risk analysis and management in organization, providing adequate training and seminars.

Appropriate set of policy Instruments: In addition to the Law on Information Security, the Strategy for the Development of Information Security and its accompanying action plan, as well as a number of key regulations (bylaws) adopted for specific actions within the field of cybersecurity the strategy also provides a list of legislative documents that additionally relate to the cybersecurity framework. These include: law on the organization and competences of public bodies in the fight against high-tech crime; penal code; law on classified data; Law on the protection of personal data; law on electronic communications; law on ratification of the convention on high-tech crime and its additional protocol; law on ratification of the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse; and the law on military security and military intelligence agency.

One envisioned activity in terms of legislative development includes establishment of a cybersecurity governance system within operators of ICT systems of special importance.

Additionally, the strategy envisions further development of the legislative framework and competences of the Office of the National Security Council and Classified Information Protection in the field of classified information protection in ICT systems, in line with appropriate EU directives, with special focus on determining competencies and regulating the process of accreditation of ICT systems for processing classified information.

Clear leadership, roles and resource allocation: The Ministry of Trade, Tourism and Telecommunications is the competent body for cybersecurity. The strategy does not explicitly list other relevant institutions, with the exception of the national CERT.

In addition, the strategy refers to the Government Body for Coordination of Information Security Affairs, established by the Law on Information Security. The body has an advisory role and reports directly to the government. It is composed of representatives of the following institutions and bodies: Ministry of Trade, Tourism and Telecommunications; General Secretariat of the Government; Ministry of Defence; Ministry of Interior; Ministry of Foreign Affairs; Ministry of Justice; Security-Intelligence Agency; Military Security Agency; Military Intelligence Agency; Government Office for Information Technologies and eGovernment; Office of the National Security Council and Classified Information Protection; and Regulatory Agency for Electronic Communications and Postal Services.

In terms of resource allocation, this can be inferred from the action plan for implementation of the strategy. The action plan lists the general goal for each strategic objective, along with an indicator of effect, initial value/situation, aimed value/situation, and verification source. These are further broken down by activity description, deadline for realisation, indicator, lead institution, partners, and sources of financing. The action plan covers the period from 2018 to 2019, although it was adopted in in August 2018. The deadlines set are mostly for the year 2018, with the exception of activities that are to take place on a continuous basis.

Trust environment: The strategy states that the legal provision enabling establishment of the expert working group within the government body for Coordination of Information Security Affairs with academic (and therefore public-private) cooperation is intended to enable development of permanent trust among all actors within the information security framework. This includes the public sector, that is, representatives of state institutions; the private sector; that is, the economy; and citizens organized into civil society.

GOOD PRACTICE

- Governance: The competent ministry in charge of cybersecurity is the Ministry of Trade Tourism and Telecommunications. The national CERT is hosted by the Regulatory Agency for Electronic Communications and Postal Services (RATEL). In addition to being in charge of developing legislation and strategic documents, the ministry also hosts an information security inspection competence, in charge of continuously monitoring the state of cybersecurity. The national CERT is tasked with developing analyses of risks and incidents in cyberspace.
- Furthermore, the Government Body for Coordination of Information Security Affairs gathers representatives of a number of relevant institutions and bodies and has an advisory role, reporting directly to the Prime Minister.

- The specialized organizational unit for high-tech crime within the Ministry of Interior and the Special Prosecutor's Office for High-Tech Crime are listed as being in charge of matters pertaining to the fight against high-tech crime, while the Office of the National Security Council and Classified Information Protection is listed as competent in the field of classified data. The Ministry of Defence and the armed forces are in charge of developing cyber defence capacities and capabilities.
- When it comes to the protection of children online, the Ministry of Trade, Tourism and Telecommunications runs a National Contact Centre for Child Safety on the Internet, as a unique contact point for providing advice and receiving reports when it comes to this issue.
- Engagement of academia and the private sector is recognized as beneficial in the field of developing solutions and systems for improving national information security, providing good practice examples and capacity building.
- Risk management in national security: In terms of sectoral policies, the strategy places specific focus on systems of special importance (essential services), or critical infrastructure. To this end, identification of critical information infrastructure is envisioned, especially following adoption of the Law on Critical Infrastructure in 2018.
- Cyber defence is also an aspect the strategy highlights, whereby establishment of information security and the ability to perform defence in cyberspace, within the effective use of forces and functional capabilities of the Serbian Armed Forces as the main subject of the defence system, is envisioned. Engagement of the Ministry of Defence and the armed forces in providing support to operators of ICT systems of special importance in terms of discovering threats and responding adequately is also mentioned.
- Children's safety online is also one of the strategic priorities of the document. To this end, referring to the UN Convention on the Rights of the Child, and the EU Strategy for a Better Internet for Children, the strategy highlights the General protocol for the protection of children from abuse and neglect the Government adopted in 2005, and the Regulation on the safety and protection of children in the use of information and communication technologies adopted in 2016. Future planned activities include raising the role and capacities of the Contact Centre for Child Safety on the Internet, including coordination of support provided in each reported case and coordination of establishment of new systemic solutions for recognized challenges.
- Preparedness and resilience: The strategy highlights that the law on information security leaves potential for the establishment of independent, special CERTs focused on prevention and protection from security risks in ICT systems within a given legal entity, group of legal entities, field of work and the like. All special CERTs are to be registered with the national CERT in order for a network of CERTs to be established for efficient information and experience exchange.
- Furthermore, alongside the national CERT, other public body CERTs have also been established or are in the process of establishment. This includes the GOV CERT, hosted by the Government Office for Information Technologies and eGovernment; CERT MUP, which is the CERT of the Ministry of Interior; BIA CERT, which is in the process of formalization as the CERT of the Security-Intelligence Agency, and a CERT of military bodies. In terms of special CERTs, six have thus far registered with the national CERT, according to SRB CERT's website, both commercial and non-profit.

- In addition to the strategic framework, the law on information security determines the obligation of all ICT operators of special importance to adopt a security act which is to determine measures of protection as well as the principles, ways and procedures for achieving and maintaining adequate level of security of systems, and competences and responsibilities for the security and resources of these entities.
- Critical infrastructure services and essential services: The strategy highlights that, according to the law on information security, ICT systems of special importance are to report all incidents in their systems that could have a significant effect on information security.
- Public-private cooperation is recognized as a beneficial framework throughout the strategy, and the document refers to the legislative provisions that enable establishment of special working groups within the Government Body for Coordination of Information Security Affairs. To this end, public-private cooperation, encompassing engagement of actors from the private, academic and civil sector, is seen as enabling timely information and resource exchanges, as well as efficient communication and optimisation of future activities.
- Capability and capacity building and awareness raising: The strategy states that the national CERT is in charge of awareness raising among private legal entities, acknowledging that cooperation with the non-governmental sector, academic community and other subjects in this field is of great importance in this endeavour. These awareness raising efforts are to focus on private sector actors on the need to apply security measures, in line with national and international standards, as well as the benefits of establishing special CERTs.
- Additional awareness raising efforts are envisioned in the specific field(s) of personal data protection, cybercrime and the safety of children online.
- In terms of capacity building, the document states that it is of extreme importance to focus on capacity building of the competent ministry in terms of inspection, as well as receiving and processing incident reports, and that of other relevant institutions.
- Establishing the basis for increased capacity of society in general is also one of stated strategic priorities. To this end, the National Education Council initiated the drafting of guidelines for increasing the role of information and communication technologies in education. The guidelines, sorted by level of urgency, focus on development strategies (long-term planning, primarily adopting necessary legislation and monitoring contemporary trends), educational institutions (recommendations applied at the institutional level), and teaching practice (recommendations pertaining to the work of teaching staff. Cross-sectoral cooperation is recognized as key in this field generally aimed at increasing interdisciplinary competences and digital literacy, targeting children and young adults in the primary and secondary level(s) of education. Introduction of special study programmes at university level is also envisioned.
- Public-private cooperation is recognized as contributing to industrial research and innovations in the field of information security. The strategy states that cooperation of the academic community with competent institutions, with active participation of the private sector, should be institutionalized to enable joint activities aimed at developing products, processes and services for ensuring adequate levels of information security. Encouraging cooperation between the scientific communi-

ty and the private sector is seen as a method for contributing to the development of technologies and services in line with recognized international standards.

- Legislation and regulation: In addition to measures pertaining directly to cybersecurity, the strategy also contains measures that focus on the fight against cybercrime. Inclusion of such measures into the strategy was seen at the time of its adoption as a temporary measure, until a separate, cybercrime strategy is adopted. To this end, the strategy for the Development of Information Security envisions capacity building activities in the field of cybercrime, namely for competent authorities - the specialized organizational unit for high-tech crime within the Ministry of Interior and the Special Prosecutor's Office for High-Tech Crime - to upgrade operational tools and operational capability for suppressing these types of criminal offenses. The necessity of improving coordination and common approaches of bodies competent for the discovery and prosecution, from the public and private sector, is also recognized. Within this activity. Continued provision of training programmes for judges dealing with instances of cybercrime, is also envisioned. The strategy emphasises that Serbia has ratified the EU Convention on Cyber-crime in 2009, which is reflected in the Law on Organization and Jurisdiction of State Authorities for Combating High-Tech Crime, as well as in provisions of the criminal code.
- International cooperation. Contact with international partners is defined as multi-layered, active and optimal, encompassing a wide array of state, non-governmental and international organizations at the political, technical and expert level. The strategy defines the following key international partners as: the United Nations (UN), Organization for Security and Cooperation in Europe (OSCE), European Union (EU), Council of Europe (CoE), political, economic, security and defence organizations and alliances with which Serbia has standing cooperation agreements, as well as neighbours and traditional allies of the country.[13] Two public body CERTs are members of Trusted Introducer - the national CERT, SRB-CERT[14] and the CERT of the Ministry of Interior, CERT MUP[15].
- Within the aspect of international cooperation, the strategy further explicitly lists the aim of active participation in international civilian and military exercises aimed at establishing and developing information security at all levels.
- International cooperation is also recognized as necessary in the field of the fight against cybercrime. To this end, two contact points for international cooperation and emergency reaction in this field have been identified - one being the special prosecutor for high-tech crime, and the other within the unit for high-tech crime within the Ministry of Interior.

[13] To date, Serbia has taken part in the fifth iteration of the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security process. It also takes an active part in the OSCE Informal Working Group on Cybersecurity, currently sponsoring the 9th OSCE Confidence-Building Measure (CBM) focused on reaching a consensus glossary of terms used in cybersecurity among member states.

[14] Listed since 1 November 2017.

[15] Accredited since 23 November 2018.

DCAF Geneva Centre for Security Sector Governance

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacitybuilding of both state and non-state security sector stakeholders.

DCAF's Foundation Council is comprised of representatives of about 60 member states and the Canton of Geneva. Active in over 80 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
☎ Tel: +41 22 730 94 00
✉ info@dcaf.ch
www.dcaf.ch
@DCAF_Geneva