CYBERSECURITY CAPACITY REVIEW

Republic of Kosovo

March 2020

Global Cyber Security Capacity Centre
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD
KWPF KOREA-WORLD BANK PARTNERSHIP FACILITY
KISA Korea Internet & Security Agency
GCCD Global Cybersecurity Center for Development
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Jakob Bund, Dr Patricia Esteve-Gonzalez

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

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*27 October 2019*	*First draft submitted to the GCSCC Technical Board*
2	*11 November 2019*	*Second draft submitted to the World Bank Group*
3	*26 November 2019*	*Third draft submitted to World Bank for circulation to the Government of the Republic of Kosovo*
4	*3 February 2020*	*Fourth draft submitted to the Government of the Republic of Kosovo for final stakeholder input*
5	*17 February 2020*	*Fifth draft submitted to the Government of the Republic of Kosovo incorporating MIA input*
6	*6 March 2020*	*Final draft submitted to the Government of the Republic of Kosovo incorporating MED and MIA input*
7	*24 March 2020*	*Proofread report submitted to the World Bank Group and the Government of the Republic of Kosovo for publication*

LIST OF ABBREVIATIONS

AIS	Agency of the Information Society (of Kosovo)
AKI	Kosovo Intelligence Agency
API	Application Programming Interface
ARKEP	Regulatory Authority of Electronic and Postal Communications
ATK	Tax Administration of Kosovo
CERT	Computer Emergency Response Team
CERT-KSF-RKS	CERT of the Kosovo Security Forces
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIS	Commonwealth of Independent States
CMM	Cybersecurity Capacity Maturity Model
CNI	Critical National Infrastructure
CoE	Council of Europe
DILC	Department of International Legal Cooperation
ECDL	European Computer Driving Licence
ECTEG	European Cybercrime Training and Education Group
eIDAS	EU Regulation on Electronic Identification and Trust Services for Electronic Transactions
EMA	Emergency Management Agency
ENCYSEC	Enhanced Cyber Security project (of the European Union)
ENISA	EU Agency for Cybersecurity
EU	European Union
EULEX	EU Rule of Law Mission in Kosovo
GCSCC	Global Cyber Security Capacity Centre
GDPR	EU General Data Protection Regulation
IANA	Internet Assigned Numbers Authority
ICITAP	International Criminal Investigative Training Assistance Program
ICK	Innovation Centre Kosovo
ICMM	Independent Commission for Mines and Minerals (of Kosovo)
IcSP	EU Instrument contributing to Stability and Peace
ICT	Information and Communications Technology

IMC	Independent Media Commission (of Kosovo)
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
KFOR	NATO Kosovo Force
KIPA	Kosovo Institute for Public Administration
KODE	Kosovo Digital Economy project (of the MED)
KOS-CERT	National Cyber Security Unit of Kosovo
KOSTT	Kosovo Electricity Transmission System and Market Operator
KP	Kosovo Police
KSC	Kosovo Security Council
KSF	Kosovo Security Forces
MED	Ministry of Economic Development of the Republic of Kosovo
MEST	Ministry of Education, Science and Technology of the Republic of Kosovo
MIA	Ministry of Internal Affairs of the Republic of Kosovo
MLAT	Mutual Legal Assistance Treaty
MoJ	Ministry of Justice of the Republic of Kosovo
NAPPD	National Agency for the Protection of Personal Data (of Kosovo)
NCS	National Cybersecurity Strategy
NCSC	National Cybersecurity Council (of Kosovo)
NGO	Non-Governmental Organisation
NIS Directive	EU Network and Information Security Directive
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
PhD	Doctor of Philosophy
PKI	Public Key Infrastructure
PPRC	Public Procurement Regulatory Commission (of Kosovo)
RTIR	Request Tracker for Incident Response
SCADA	Supervisory Control and Data Acquisition System
SIEM	Security Information and Event Management System

SMEs	Small and Medium-sized Enterprises
SOC	Security Operations Centre
STIKK	Association for Information Technology and Communication of Kosovo
TLD	Top-level Domain
UBT	University for Business and Technology
UNDP	United Nations Development Programme
USAID	US Agency for International Development
VET	Vocational Education and Training
WBG	World Bank Group

EXECUTIVE SUMMARY

In collaboration with the World Bank, the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a second review of the maturity of cybersecurity capacity in Kosovo at the invitation of the Ministry of Economic Development (MED). This assessment follows an earlier baseline assessment against the Cybersecurity Capacity Maturity Model (CMM) conducted by the Centre in 2015.[1] As in 2019, the 2015 assessment was hosted by the Ministry of Economic Development of the Republic of Kosovo (MED) and facilitated by the World Bank Group (WBG). The objective of this follow-on review was to enable Kosovo to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities, and to help measure progress in implementing the recommendations from the 2015 review.

Over the period 16–19 July 2019, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology (IT) officers and representatives from public-sector entities, critical-infrastructure owners, policy makers, IT officers from the Government and the private sector (including financial institutions), telecommunications companies, and the banking sector, as well as international partners.

The consultations took place using the Centre's CMM, which defines five *dimensions* of cybersecurity capacity:

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

Each *dimension* contains a number of *factors* which describe what it means to possess cybersecurity capacity in that *dimension*. Each *factor* presents a number of *aspects* grouping together related *indicators*, which describe steps and actions that, once observed, define the stage of maturity of that *aspect*. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The *start-up* stage implies an *ad-hoc* approach to capacity, whereas the *dynamic* stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[2]

[1] The full assessment report of the 2015 review is available online: Maria Bada, "Cybersecurity Capacity Assessment of the Republic of Kosovo," *Global Cyber Security Capacity Centre*, June 2015, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-cybersecurity-capacity-review-2015.

[2] Global Cybersecurity Capacity Centre, **"**Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition" February 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

Figure 1 below provides an overall representation of the cybersecurity capacity in Kosovo in 2019 and illustrates the maturity estimates in each *dimension*. Each *dimension* represents one-fifth of the graphic, with the five stages of maturity for each *factor* extending outwards from the centre of the graphic; *start-up* is closest to the centre of the graphic and *dynamic* is placed at the perimeter.

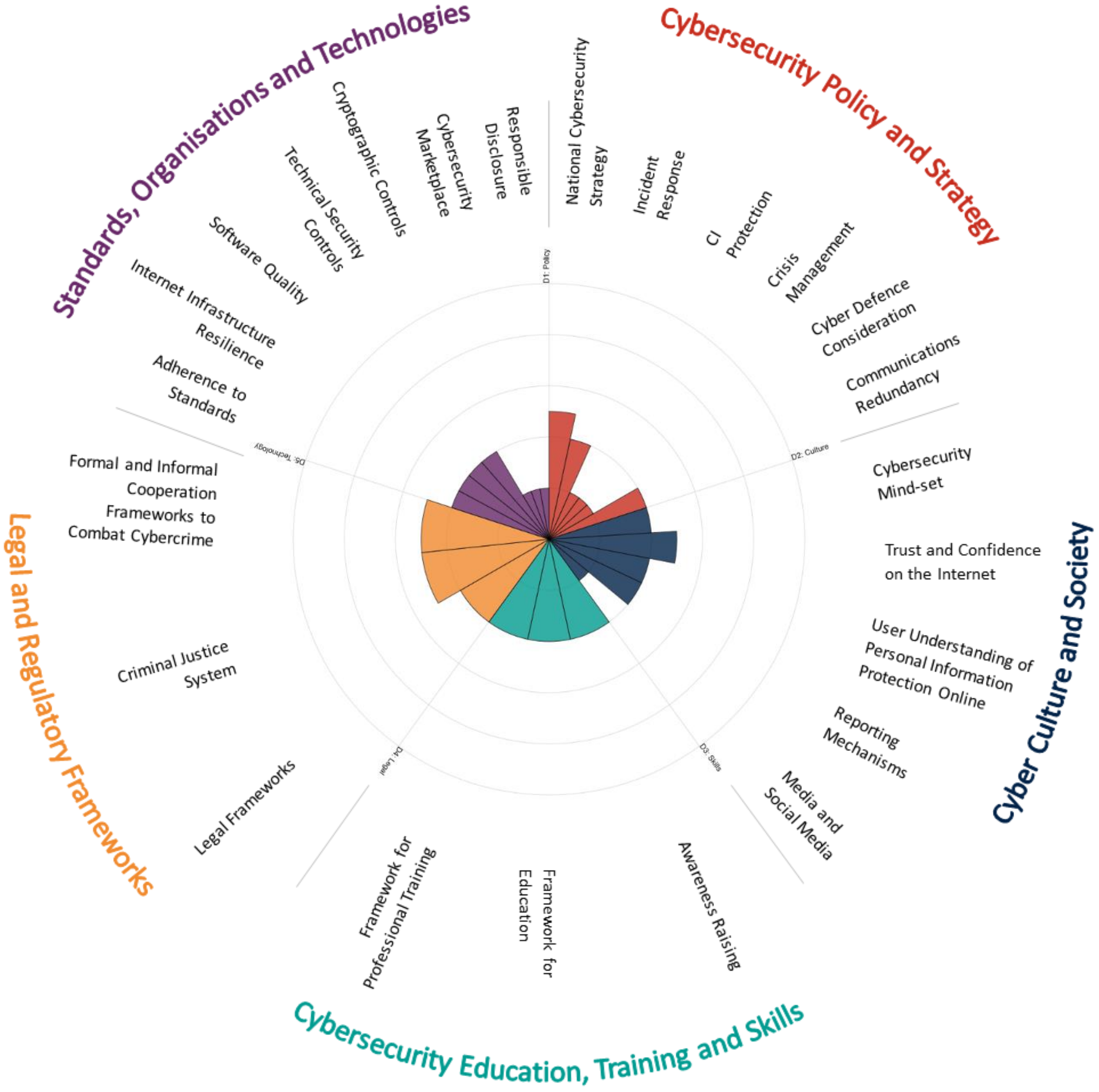

Figure 1: Overall representation of the cybersecurity capacity in Kosovo

Cybersecurity Policy and Strategy

In June 2015, the Government of Kosovo issued the formal decision to set up a multi-stakeholder working group to begin the development of Kosovo's first National Cybersecurity Strategy (NCS), designating the Ministry of Internal Affairs (MIA) as lead entity. The strategy and an action plan supporting its implementation through to 2019 were adopted in 2016. Based on the NCS, Kosovo has created a National Cybersecurity Council (NCSC) as a coordination platform for stakeholders involved in the implementation of the Strategy. The NCS further established the role of National Cybersecurity Coordinator, who chairs the NCSC and is charged with coordinating, monitoring and reporting on the implementation of the NCS. Under the current NCS, these responsibilities are delegated to the MIA. In addition to the NCS, two other important planning documents address implications of technology and guide a related policy in Kosovo. The first of these is the *Digital Agenda for Kosova 2013–20*, which precedes and outlives the first NCS and sets a policy for the electronic communication sector. The second planning document, concerning technology policy, is Kosovo's *IT Strategy*, focused on developing domestic and overseas markets for Kosovar companies providing IT services. Steps for the preparation of a follow-on NCS are currently underway under the leadership of the MIA.

Since July 2016, Kosovo has been operating a national cyber-incident response unit, the National Cyber Security Unit of Kosovo (KOS-CERT), which is structurally integrated into the Regulatory Authority of Electronic and Postal Communications (ARKEP). KOS-CERT is tasked with technical incident response and awareness-raising. However, no explicit mandate defining responsibilities and duties has been awarded to KOS-CERT. At the time of this assessment, KOS-CERT faced a severe personnel shortage and was only operated by two staff members. KOS-CERT receives a relatively low number of direct incident reports, which the team attributes to insufficient capacities of institutions to detect incidents. Around 50 incident-response teams operate across Kosovo, including ministries, government agencies and private-sector organisations—such as major banks and Internet service providers (ISPs)—with select ISPs running or setting up three-tier security operations centres (SOCs). Levels of competency and capacity vary significantly among these units, with only a small proportion being able to independently detect incidents. No general incident-reporting requirements exist by law in Kosovo. Provisions within the 2012 *Law on Electronic Communications* have allowed ARKEP to set requirements for electronic communication network and service providers to report to it any breach of security or loss of integrity that is expected to have a significant impact on the continued operations of their networks or services.

In 2018, Kosovo adopted the *Law on Critical Infrastructure* based on European Union (EU) legislation for the identification and designation of critical infrastructure. The law relies on sub-legal acts for implementation and only provides procedures for the identification and designation of critical national infrastructure (CNI) operators. The MIA is leading the process for identifying CNI under the law, in wider stakeholder consultations and following a comprehensive risk analysis that evaluates the potential disruption or destruction of critical infrastructure and its impact on the economy, society and political stability. In parallel, the MED is undertaking efforts to transpose the EU Network and Information Security Directive (NIS Directive).

The NCSC, Kosovo’s main coordinating body for cybersecurity policy, presently holds no mandate to prepare or coordinate a joint action to manage the response to a national-level crisis. The 2011 *Law for Protection against Natural and Other Disasters*, in its definition of “other disasters”, includes a specific mention of extraordinary emergency situations involving telecommunications and IT. The law designates the Emergency Management Agency (EMA) under the MIA as the responsible body for developing a national disaster recovery plan. This plan remains to be tested in the scenario of a national-level cyber-incident. Institutional capacities have been tested in individual national and international exercises. The 2018 edition of the Silver Sabre Exercise conducted by KFOR, the NATO-led peacekeeping force deployed in Kosovo, contained elements for the test of emergency-response assets in the face of a cyber-incident.

The Kosovo Security Forces (KSF) set up a computer emergency response team (CERT) in 2015. This team is presently composed of only a single member, after the rotation in assignments recently reduced the headcount from three. KSF plans to raise this number to 15 but will likely run into recruitment difficulties or will have to invest additional time in training up the qualified personnel. The CERT of the Kosovo Security Forces (CERT-KSF-RKS) reports to the Minister of Defence as the director of the CERT and is officially tasked with managing cyber-incidents to provide mission assurance in protecting information systems and services of the KSF.

Electronic communications network and service providers are required to develop and submit a plan to ARKEP detailing measures to ensure the integrity and continued availability of public communication networks in the event of serious network damages, natural disasters or emergencies in a state of war. Measures undertaken under this plan need, in particular, to ensure the uninterrupted access and use of emergency numbers. Within their respective remits, central and local government authorities are responsible for building and maintaining electronic communication capacities as part of a dedicated communication system that enables emergency and rescue services to continue their work in the event of a wider collapse of communication networks.

Cyber Culture and Society

Kosovar society, as a whole, appears to be taking steps towards extending good cybersecurity practices to the majority of its members. Internet penetration is extended over Kosovo but only a limited proportion of Internet users (younger generations) have a more advanced and proactive cybersecurity mind-set. Similarly, some leading agencies in the Government and the industry have introduced good practices after the identification of cyber threats and risks. There is, however, a need to build cybersecurity good practices at all levels of Government and across all industry sectors, and to elevate the priority of developing a cybersecurity mind-set.

Trust and confidence in the Internet have grown over the last four years, especially with regard to e-commerce and e-government services. Online payments are not very commonly used in Kosovo and there is only one main firm offering e-commerce services. However, the customer-oriented service provision of this firm—which raises awareness among users about security risks related to online shopping and measures to help protect themselves—is fostering user trust in the secure use of e-commerce services. With respect to e-government services, private-sector and Government representatives acknowledge that investment in the digitalisation process of government services requires a proportional investment in security measures.

Internet users are perceived to have minimal knowledge of how personal information is handled online. The National Agency for Protection of Personal Data supervises the implementation of the *Law on Personal Data Protection*, does receive individual complaints regarding suspected violations of personal data protection rights, and promotes public awareness on this topic. However, the agency's resources remain insufficient for it to fulfil its mandate.

Several channels exist to report cyber-enabled incidents but these are not commonly used by victims of cybercrime. Most Internet users are not aware of the existing reporting mechanisms, and victims usually report to the nearest police office or, in cases involving a particular social media platform, directly to the platform.

Cybersecurity issues are rarely covered in the media or on social media, and stakeholders have identified enhanced efforts by the media industry towards raising cybersecurity awareness as an area for improvement.

Cybersecurity Education, Training and Skills

Interviewed participants highlighted the need to intensify efforts to raise awareness of cybersecurity risks and threats across different sectors of the Kosovar society. The action plan accompanying the National Cybersecurity Strategy foresees differentiated awareness campaigns specifically designed to the needs of various sub-communities of users, including younger generations and Government employees. However, these efforts need to be coordinated and would benefit from partnerships with gateway institutions, such as ISPs. Executives of small and medium-sized enterprises (SMEs), who often serve as CEO, CIO and CISO at the same time, represent a particularly important outreach audience.

Curricula for the pre-university education system of Kosovo include information and communications technology (ICT) competences and the responsible use of technology and online services. However, schools face problems in integrating ICT-related competences in their teaching. Not all schools in Kosovo have ICT equipment, and institutions with access often only have a limited number of teachers available with the know-how to leverage ICT equipment in class. The Ministry of Education, Science and Technology has detected these shortcomings and has unrolled a strategic plan supported by a dedicated budget to address them.

Universities, higher education centres and vocational schools in Kosovo offer a wide range of study programmes in fields related to cybersecurity at various levels. In addition, private-sector offerings provide training programmes both for cybersecurity specialists and the general work force. Finally, qualification systems exist for ICT professionals, although programmes tend to be based on a partial or custom adaptation of international standards. Overall, despite the wide range of higher education programmes and comparatively high rates of uptake, ICT security courses remain limited. The resulting shortage of ICT professionals is in part exacerbated by incentives for graduates to seek out employment opportunities abroad that offer more competitive remuneration. This shortage, in turn, affects the limited availability of experts who can train ICT professionals.

Legal and Regulatory Frameworks

At the time of this assessment, Kosovo had not yet enacted any overarching law concerning ICT security specifically. At the sectoral level, the *Law on Electronic Communications*, adopted in 2012, addresses select ICT security aspects with a narrower focus on operators of electronic communications networks and service providers. The law vests the ARKEP with the authority to issue regulations on technical and organisational security measures and set auditing and breach notification requirements.

The MIA is working on a new comprehensive cybersecurity law with ambitions to also overhaul the 2010 *Law on the Prevention and Fight of Cybercrime*. Freedom of expression online is not explicitly regulated in Kosovo. Fundamental rights, including freedom of speech, however, are regularly referenced in legislation on electronic communications or digital data protection as foundational building blocks.

In February 2019, Kosovo enacted a new *Law on Protection of Personal Data* that aspires to be a full transposition of the EU General Data Protection Regulations (GDPR) and reinforces the role of the National Agency for the Protection of Personal Data (NAPPD) in promoting and supporting fundamental rights on personal data protection. Under the law, data breaches generally need to be reported to the NAPPD. This agency is legally empowered to impose fines for non-compliance in line with GDPR provisions. Based on its own reporting, the NAPPD is operating under severe budgetary constraints and with a low staff count that do not allow for all agency departments to operate as foreseen by the agency's institutional charter. At the time of this assessment, the agency had not been able to conduct compliance inspections for three years.

In June 2019, the National Assembly adopted a new *Law on Child Protection*, which is set to enter into force in June 2020. Sections of the law pertaining specifically to child protection online primarily concern access limitations and advisories on potentially harmful content, including steps to close off online gambling platforms to minors. The law requires electronic and online media and Internet portals to actively implement child-protection measures, including awareness-raising efforts to inform on potentially negative effects of exposure of children to certain media products.

Kosovo adopted a new *Law on Consumer Protection* in June 2018, which effectively transposes EU legislation on consumer protection. The present law does not contain any provisions particularly addressing consumer protection online but could be applied, drawing on established practices in EU member states for implementing and enforcing the transposed EU Directives on which Kosovo's *Law on Consumer Protection* is based.

An array of laws regulates various aspects of intellectual property protection severally, including the *Law on Copyright and Related Rights*, the *Law on Patents*, the *Law on Industrial Design* and the Criminal Code. These laws are not specific to the protection of intellectual property online but are broad in scope and admit general application independent of the medium.

In 2010, Kosovo enacted the *Law on the Prevention and Fight of Cybercrime*, which serves as the main legal text on substantive matters of cybercrime. While Kosovo is not a signatory to the Convention on Cybercrime of the Council of Europe (CETS No. 185) (Budapest Convention), a section-by-section comparison prepared by the Council of Europe (CoE) within the framework of the organisation's capacity-building programmes shows that all core components of the Budapest Convention have been codified into the law. In the view of several of the stakeholders consulted, including government officials and international partners, the present cybercrime law addresses only a minimal set of cybercrimes and cyber-enabled criminal offences and is considered in need of revision to reflect technological advances and related evolutions in criminal behaviour. Procedural aspects of Kosovo's cybercrime legislation are largely codified in the Criminal Procedure Code.

The KP operates a specialised unit under the Directorate for Investigation of Organised Crime that is tasked with the investigation of cybercrime. The Kosovo Forensic Agency lends additional investigatory support with the evaluation of electronic evidence. The *Law on the Prevention and Fight of Cybercrime* recognises the need for continuous training of investigators, prosecutors and members of the judiciary who are charged with fighting cybercrime. Kosovo was one of the beneficiaries of the Cooperation on Cybercrime under the Instrument of Pre-accession (IPA) project (iPROCEEDS), funded by the EU and the CoE, that organised training and consultations aimed at strengthening legislation and the ability of authorities to search and seize gains from cybercrime. Judges and prosecutors are required to take part in annual professional training, which includes options on cybercrime. Since 2016, the Academy of Justice has been conducting a specialised multi-session training programme to bolster capacity for combatting cybercrime on an annual basis.

Kosovo's overarching *Law on International Legal Cooperation in Criminal Matters*, which regulates mutual legal assistance, also extends to cooperation to combat cybercrime. Formal requests for legal cooperation are generally placed and processed on a basis of mutual legal assistance treaties (MLATs). The Department of International Legal Cooperation (DILC) within the Ministry of Justice serves as the central point of contact for mutual legal assistance in criminal matters. Kosovo has not yet set up a 24/7 point of contact. Requests for the police can, however, be submitted on an informal basis to the Directorate for International Cooperation in the Rule of Law of the KP. Assistance between Kosovo authorities and ISPs is widely codified. Kosovo's main ISPs are reported to have designated a data protection officer specifically to respond to law enforcement requests for access to customer data, and to act only on the basis of a judicial authorisation.

Standards, Organisations, and Technologies

Uptake of international ICT security and risk-management standards varies widely between private and public sector organisations in Kosovo. Standardisation efforts tend to focus on developing policies and harmonising practices within the organisation. Only a subset of domestic organisations and local companies moves on to external guidance, mostly ISO resources. In 2016, ARKEP issued regulations specific to network and electronic service providers based on authority conferred by the *Law on Electronic Communications*. In addition to introducing minimum technical and organisational standards for security and integrity, the requirements order certain operators to conduct regular independent security audits and to share results with the overseeing regulator.

The *Law on Public Procurement* delineates spending criteria for public funds. The law does not contain direct mentions of the role of ICT security in procurement decisions. Provisions include the option to review bids based on their technical merits but establish no legal requirements to make the consideration of ICT security standards an integral part of tender specifications.

No coherent approach or well-defined frameworks specific to software development are being promoted by the Government. As a result, the bulk of software development needs is being contracted out. In practice, the software-development methodologies applied consider integrity and resilience in as much as they are embedded in external application programming interfaces (APIs) that often form the foundation of many projects.

Three main ISPs connect users and businesses in Kosovo to international Internet gateways. Connectivity for the last mile is provided by 51 smaller regional operators. Notable regional divides exist with regard to fixed broadband penetration. In particular, districts in the southwest and in the north of Kosovo have penetration rates that fall significantly below the national average. ISPs are obliged to provide information to ARKEP, about the equipment they deploy. For the past years, these obligations have been observed for telephone landlines and mobile networks. In 2019, these rules, for the first time, will be applied to infrastructure that supports fixed-Internet connections. In addition, ISPs are required to conduct impact assessments of any incidents occurring on their networks based on the framework provided by ARKEP.

Kosovo’s major ISPs have developed and implemented policies for patch management and for maintaining systems under their supervision. These policies have been extended to include third-party suppliers. For many other businesses, however, especially outside the ICT security market, systematic checks for and application of security updates are not a high priority in light of resource constraints. Widespread use of pirated software fundamentally limits access to security updates.

Based on a comparative review of industry practices conducted by local university researchers, financial institutions lead in the adoption of technical security controls nationally and follow global standards to maintain international business and access to banking networks. Software-development companies were found which could implement network security measures to facilitate the early detection of intrusions but appeared to be lacking in strategic planning for data backups. KOS-CERT, which has received the first instalment of security audits from ISPs, assessed that, on the whole, ISPs marshal the technical and human capacity to put appropriate security controls in place, supported by a backup policy. Major ISPs maintain upstream filtering of malicious content and offer additional security services, including protection against denial-of-service attacks.

Kosovo’s larger ISPs and telecommunication companies encrypt sensitive data at rest and manage employee access on a restrictive need-to-know basis. At least one major software-development and engineering company consulted for this assessment, however, reported a general absence of cryptographic requirements in their contract work. With respect to user behaviour, private-sector representatives assessed that older generations, while used to prolific practices of surveillance by analogue means in the past, did not generally apply the same precautious mind-set in their use of networked devices or online services. Younger generations, by comparison, showed greater appreciation of the privacy and data protection concerns linked to online activities.

IT firms in Kosovo share a strong export orientation, with close to half of the surveyed companies naming overseas markets as their primary customer base. The limited size of the domestic technology ecosystem only offers restricted potential to scale up for local companies, leading them to seek out more profitable contracts abroad. Several companies offer penetration-testing services domestically. The identification of the need for cybersecurity insurance remains largely confined to banks and concerns related to financial losses due to cybercrime. Representatives from other industries in the private sector stated that they were not aware of any cybersecurity insurance offerings that catered specifically to the market in Kosovo.

Currently, no frameworks or institutionalised channels exist for the responsible disclosure of security flaws to government agencies. None of the companies consulted for this assessment were operating a mechanism for responsible disclosure or could identify an entity with such a framework in place.

INTRODUCTION

At the invitation of the Ministry of Economic Development (MED) and in collaboration with the World Bank Group (WBG), the Global Cyber Security Capacity Centre (GCSCC or 'the Centre') has conducted a second review of cybersecurity capacity of Kosovo. This assessment follows an earlier baseline assessment against the CMM conducted by the Centre in 2015.[3] As in 2019, the 2015 assessment was hosted by the MED and facilitated by the WBG. The objective of this review was to enable Kosovo to determine areas of capacity in which the Government might strategically invest in, in order to improve their national cybersecurity posture. In addition to providing updated analysis of Kosovo's cybersecurity capacity stack, this 2019 assessment offers comparative perspectives on progress that has been achieved since the 2015 review in further developing these capacities, highlighting areas of capacity advancement, areas of consolidation and enduring challenges.

Over the period 16–19 July 2019, stakeholders from the following sectors participated in a three-day consultation process:

Government ministries, agencies and legislative bodies:

- Agency for the Information Society (AIS)
- Assembly of the Republic of Kosovo–Committee for Education, Science, Technology, Culture, Youth, Sports, Innovation and Entrepreneurship
- Assembly of the Republic of Kosovo–Committee on Economic Development, Infrastructure, Trade, Industry and Regional Development
- CERT of the Kosovo Security Forces (CERT-KSF-RKS)
- Kosovo Intelligence Agency (AKI)
- Ministry of Economic Development of the Republic of Kosovo
- Ministry of Finance of the Republic of Kosovo
- Ministry of Health of the Republic of Kosovo
- Ministry of Justice of the Republic of Kosovo
- National Cyber Security Unit (KOS-CERT)
- Police Inspectorate of Kosovo
- Kosovo Security Council
- Tax Administration of Kosovo (ATK)

Finance sector:

- Kosovo Banking Association

Critical infrastructure owners and regulators:

- Artmotion
- Cable Association of Kosovo

[3] The full assessment report of the 2015 review is available online: Maria Bada, "Cybersecurity Capacity Assessment of the Republic of Kosovo," *Global Cyber Security Capacity Centre*, June 2015, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-cybersecurity-capacity-review-2015.

- Central Bank of Kosovo
- Independent Commission for Mines and Minerals (ICMM)
- IPKO
- Kosovo Electricity Transmission System and Market Operator (KOSTT)
- Kosovo Railway Company Trainkos
- Kosovo Telecom
- Kujtesa
- Regional Water Company Pristina
- Regulatory Authority of Electronic and Postal Communications (ARKEP)

Additional private enterprises:

- 3CIS
- Cacttus
- InterAdria
- Sentry Cybersecurity

Academia:

- CERT at the University of Business and Technology (UBT-CERT)
- Rochester Institute of Technology Kosovo
- University of Business and Technology

Civil society organisations:

- Bonevet
- Center for Cyber Security and Privacy
- Centre for Advanced Studies (FIT)

International community:

- United Nations Development Programme (UNDP)

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM),[4] which is composed of five distinct *dimensions* of cybersecurity capacity. Each dimension consists of a set of *factors*, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five *dimensions* together with the *factors* which each of them presents:

DIMENSIONS	**FACTORS**
Dimension 1 **Cybersecurity Policy and Strategy**	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 **Cyber Culture and Society**	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 **Cybersecurity Education, Training and Skills**	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 **Legal and Regulatory Frameworks**	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 **Standards, Organisations, and Technologies**	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

[4] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition," February 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

STAGES OF CYBERSECURITY CAPACITY MATURITY

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

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

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

The first baseline CMM assessment of Kosovo in 2015 had been conducted based on an earlier version of the CMM. In step with evolving security challenges and based on the experience of deploying the model in the field, the CMM was reviewed and updated in February 2017. The majority of these changes address the level below the *factors* outlined above and concern existing *aspects* or introduce new ones.

This revised version of the model, which was deployed for this 2019 assessment, adds a range of new aspects for analysis, such as the ‘Mode of Operation’ of the incident-response capacity in Dimension 1, ‘User Understanding of Personal Information Protection Online’, ‘Reporting Mechanisms’, reporting of cyber incidents by ‘Media and Social Media’ in Dimension 2, ‘Data Protection Legislation’, ‘Child Protection Online’, ‘Consumer Protection Legislation’, ‘Intellectual Property Legislation’, ‘Formal Cooperation’ and ‘Informal Cooperation’ on cybercrime matters in Dimension 4, and ‘Software Quality’, ‘Technical Security Controls’, and ‘Cryptographic Controls’ in Dimension 5.

A comprehensive overview, cataloguing amendments, can be found on the GCSCC website.[5]

METHODOLOGY - MEASURING MATURITY

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

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

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[6] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[7] It is this interaction and tension that offers advantage over other

[5] “CMM Revised Edition: Summary of Changes,” *Cybersecurity Capacity Portal*, 9 February 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition-summary-changes.

[6] Relevant publications: Malcolm Williams, *Making Sense of Social Research* (London: Sage Publications, 2003); John Knodel, “The Design and Analysis of Focus Group Studies: A Practical Approach,” in *Successful Focus Groups: Advancing the State of the Art*, ed. David L. Morgan (Thousand Oaks, CA: SAGE Publications, 1993); Richard A. Krueger, Mary Anne Casey, *Focus Groups: A Practical Guide for Applied Research* (London: Sage Publications, 2009).

[7] Relevant publications: Jenny Kitzinger, “The Methodology of Focus Groups: The Importance of Interaction between Research Participants,” *Sociology of Health & Illness* 16, no. 1 (1994),

methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[8]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis–a systematic research methodology used to analyse qualitative data–is applied to the data generated by focus groups.[9] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[10]

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[11] The process is repeated, and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[12] Dey explains that this process categorises data as "belonging together".[13]

The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.[14]

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

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each

https://doi.org/10.1111/1467-9566.ep11347023; Jenny Kitzinger, "Qualitative Research: Introducing Focus Groups". *British Medical Journal* 311, no. 7000 (1995), https://doi.org/10.1136/bmj.311.7000.299; Edward F. Fern, "The Use of Focus Groups for Idea Generation: The Effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality," *Journal of Marketing Research* 19, no. 1 (1982), https://doi.org/10.1177%2F002224378201900101.

[8] Kitzinger (1995).

[9] Klaus Krippendorff, *Content Analysis: An Introduction to its Methodology* (Thousand Oaks, CA: Sage Publications, 2004); Hisu-Fang Hsieh and Sarah E. Shannon, "Three Approaches to Qualitative Content Analysis*," Qualitative Health Research* 15, no. 9 (2005), https://doi.org/10.1177/1049732305276687; Kimberly A. Neuendorf, *The Content Analysis Guidebook* (Thousand Oaks, CA: Sage Publications, 2002).

[10] Fern (1982).

[11] Satu Elo et al., "The Qualitative Content Analysis Process." *Journal of Advanced Nursing* 62, no. 1 (2014), https://doi.org/10.1111/j.1365-2648.2007.04569.x; Hsieh and Shannon (2005).

[12] Barbara Downe-Wamboldt, "Content Analysis: Method, Applications, and Issues." *Health Care for Women International* 13, no. 3 (1992), https://doi.org/10.1080/07399339209516006.

[13] Ian Dey, *Qualitative Data Analysis: A User-friendly Guide for Social Scientists* (London: Routledge, 2003).

[14] See footnote 4.

factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and uses the indicators of the CMM as criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised, or to tailor the Centre's recommendations.

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

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

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

CYBERSECURITY CONTEXT IN KOSOVO

The Kosovo government has identified IT development "to become the main driver for economic growth, employment and innovation until the year 2020 by increasing the international competitiveness of the IT industry based on digital excellence."[15] This emphasis on IT in the same line underscores the importance of making cybersecurity considerations an integral part of this effort—not just to secure products and services but also to protect economic growth overall.

To this end, Kosovo has undertaken critical steps since 2015, when the GCSCC conducted a first baseline assessment applying the CMM. *Table 1* provides a summary overview of capacity developments for all factors assessed both in 2015 and 2019. Most notably, Kosovo adopted its first National Cybersecurity Strategy (NCS) in January 2016. In support of the operationalisation of the strategy, an inter-agency NCS has been formed that convenes key stakeholders involved in the implementation process and streamlines progress reporting. In addition to the council, the NCS created the role of National Cybersecurity Coordinator, to be exercised by the Minister of Internal Affairs or their designated representative. These new institutions and functions have established important structures and communication channels that offer important avenues towards closer cooperation across Government.

The NCS has given impetus to ambitious legislative reform, including the overhaul of cybercrime legislation, the development of a comprehensive umbrella *Law on Cybersecurity*, and the creation of a legal basis for the identification of critical national infrastructure (CNI). Select regulators have taken first steps to ensure the adoption of security standards and practices within the sectors they oversee. In this vein, electronic communication service providers, for instance, have been issued requirements to complete security audits and to comply with minimum technical security measures. In the cases where expertise in these efforts is sourced from international technical assistance missions, as for instance in digitalisation initiatives for the public administration, the relevant Kosovo authorities need to identify appropriately skilled counterparts to receive and process technical advice. Identifying the right subject matter experts within Kosovar institutions is key for engaging with international partners at the necessary level of detail, to take full advantage of these opportunities for knowledge transfer and ensure sustainable effects. At the same time, international partners carry a responsibility to strive for inclusiveness. In a networked ecosystem, initiatives depend on broader community consultation and "buy-in", which also serve as pathways for continued commitment to implementation and uptake by all relevant stakeholders.

[15] Ministry of Economic Development of the Republic of Kosovo, Kosovo IT Strategy, June 2016, 9, http://www.kryeministri-ks.net/repository/docs/Kosovo_IT_Strategy.pdf.

Factors based on CMM 2015*	Maturity Stage[‡]		Capacity Developments*
	2015	2019	
D1 Cybersecurity Policy and Strategy			
D1.1 National Cybersecurity Strategy	Start-up	Formative to Established	+ +
D1.2 Incident Response	Start-up	Formative	+ +
D1.3 Critical Infrastructure Protection	Start-up	Start-up	o
D1.4 Crisis Management	Start-up	Start-up	o
D1.5 Cyber Defence Consideration	Start-up	Start-up	o
D1.6 Digital Redundancy	Formative	Formative	o
D2 Cyber Culture and Society			
D2.1 Cybersecurity Mind-Set	Formative	Formative	o
D2.2 Cybersecurity Awareness	Formative	Formative to Established (*now assessed in D3.1*)	+
D2.3 Confidence and Trust on the Internet	Formative	Formative to Established	+
D2.4 Privacy Online	Established	(*now assessed as part of D4.1*)	
D3 Cybersecurity Education, Training and Skills			
D3.1 Availability of Cyber Education and Training	Formative	Formative (*now assessed in D3.2 and D3.3*)	o
D3.2 Development of Cybersecurity Education	Formative	Formative	o
D3.3 Training and Educational Initiatives within Companies	Formative	Formative	o
D3.4 Corporate Governance, Knowledge and Standards	Start-up	Start-up to Formative (*now assessed in D3.1*)	+
D4 Legal and Regulatory Frameworks			
D4.1 Cybersecurity Legal Frameworks	Formative	Formative	+
D4.2 Legal Investigation	Formative	Formative to Established	+
D4.3 Responsible Disclosure	Start-up	Start-up (*now assessed in D5.7*)	o
D5 Standards, Organisations and Technologies			
D5.1 Adherence to Standards	Formative	Formative	+
D5.2 National Infrastructure Resilience	Formative	Formative	o
D5.3 Cybersecurity Marketplace	Start-up	Start-up	o

Table 1: Capacity developments comparing CMM assessments of Kosovo in 2015 and 2019

[‡] For reasons of backward compatibility, this overview presents maturity levels observed in the 2019 CMM assessment in the framework of a previous version of the CMM that had served as the basis for the CMM review of Kosovo conducted in 2015.

[*] Factors that have seen improvements in select indicators but not sufficient progress to warrant an upgrade in the maturity level have been marked «+». Factors with a step change in the maturity level have received the mark «+ +». Any factors without notable progress have been registered with the neutral mark «o». Any regression, if observed, would have been marked «-»/«- -», correspondingly.

These considerations deserve particular attention in the context of Kosovo, as international donors play an important support function for infrastructure development and the build-up of capacity for the provision of public services. Globally, Kosovo is ranked number 23 in terms of official development assistance received per capita.[16] National cybersecurity efforts are no exception in this regard. Kosovo has leveraged international cooperation in many of the areas that showed most progress in the 2015–19 period, based on comparative observations from the GCSCC assessments.

The regional EU-funded Enhancing Cyber Security (ENCYSEC) project, for instance, reinforced momentum for the development of the NCS in 2015, providing best-practice guidance and facilitating stakeholder consultations. Given Kosovo's active donor space, coordination of funding interests and initiatives has become a critical condition for ensuring their effective contribution to capacity development. Cybersecurity-related projects offer a range of positive examples for such joint initiatives. ENCYSEC assistance in the development of the NCS has been complemented by the Organization for Security and Co-operation in Europe (OSCE) support for monitoring and evaluating the Strategy's implementation. The EU and the Council of Europe (CoE) have linked efforts under the auspices of the iPROCEEDS project to provide training to members of the police, the judiciary and prosecutors in Kosovo with the aim of strengthening investigative capacities and regional, legal cooperation on cybercrime matters. In a similar vein, the United Nations Development Programme (UNDP) and Norway have partnered to strengthen the digital forensics capabilities of the cybercrime unit within the KP and improve collaboration between the unit and the national CERT on cyber-incidents with a possible criminal dimension.

At the time of the consultations for this report, the Ministry of Internal Affairs (MIA) had undertaken first exploratory steps to prepare the next iteration of the NCS. The 2015 and 2019 reviews of Kosovo's national capacity conducted by the GCSCC have roughly coincided with the beginning of preparations of the first NCS and end of its implementation process. Embracing the life cycle of the first NCS and preceding first substantial consultations for the development of a follow-on strategy, the assessment reports in 2015 and 2019 have provided opportunities to establish baselines for Kosovo's existing capacities. Based on these findings, the GCSCC assessment reports have prepared recommendations to address enduring challenges that can inform Kosovo's NCS development process.

[16] "Net ODA received per capita (current US$)," World Bank, accessed 1 November 2019, https://data.worldbank.org/indicator/dt.oda.odat.pc.zs?most_recent_value_desc=true.

REVIEW REPORT

OVERVIEW

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

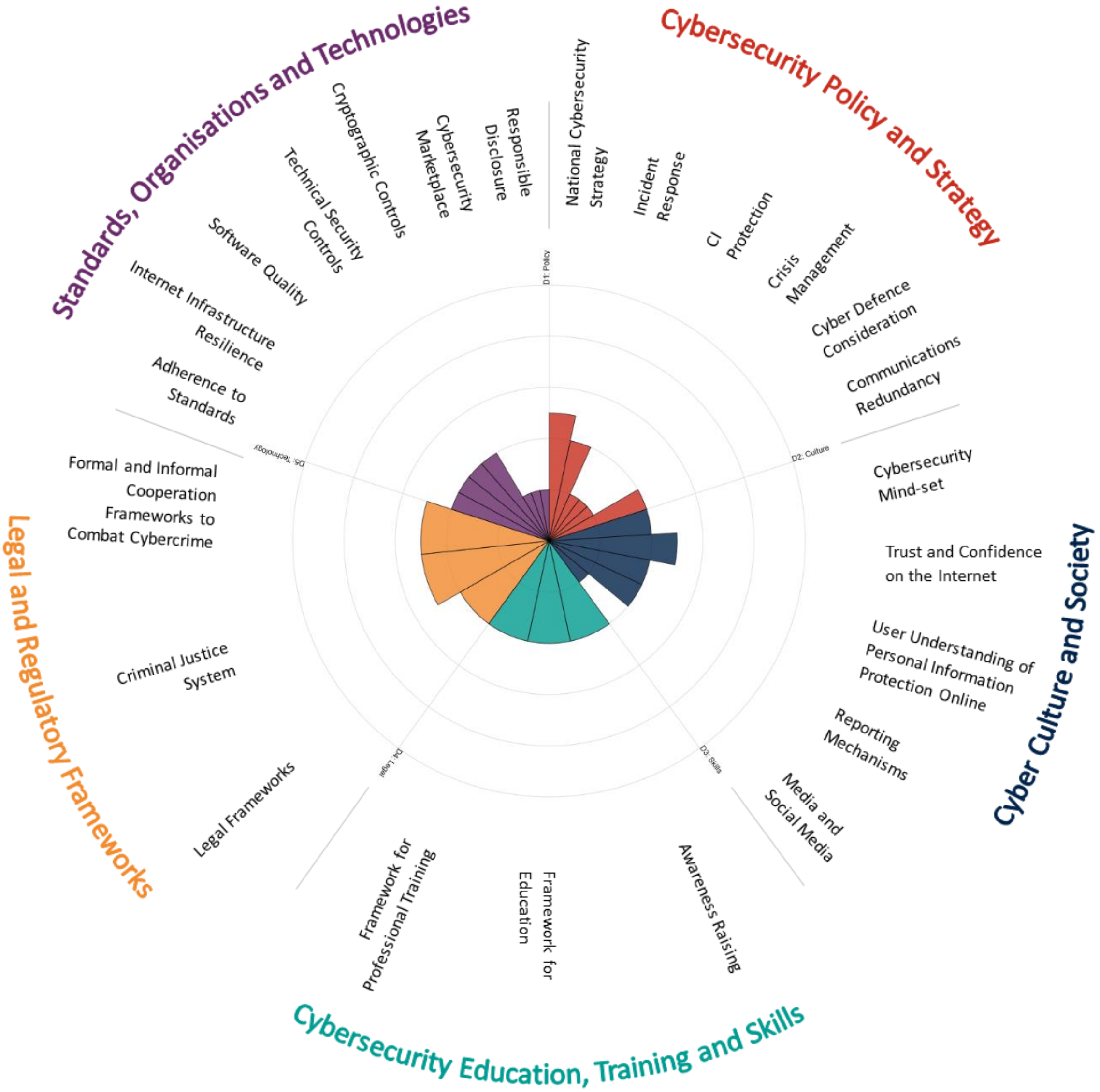

Figure 2: Overall representation of the cybersecurity capacity in Kosovo

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

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

D 1.1 NATIONAL CYBERSECURITY STRATEGY

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

Stage: Formative to Established

At the time the GCSCC conducted the first baseline CMM assessment for Kosovo, in February 2015, plans for developing a national cybersecurity strategy (NCS) were in the early stages of exploration. In its conclusion, the assessment report suggested that the Ministry of Economic Development (MED), which was responsible for overseeing the CMM review in Kosovo, would be well positioned to lead efforts for the development and implementation of an NCS.[17] This recommendation was based on the MED's existing connections with critical stakeholders, established in the preparation of the *Digital Agenda for Kosova 2013-2020* that seeks to leverage technology policy for the wider economic advancement of Kosovo. In addition, the assessment report at the time recognised the role the Ministry of Internal Affairs (MIA) played

[17] Maria Bada, "Cybersecurity Capacity Assessment of the Republic of Kosovo," *Global Cyber Security Capacity Centre*, June 2015, 36, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-cybersecurity-capacity-review-2015.

in governing and securing citizen data and underscored the importance of the close involvement of the Ministry in any effort to develop an NCS.

In June 2015, the Government of Kosovo issued the formal decision to set up a multi-stakeholder working group to begin the development of Kosovo's first NCS, designating the MIA as lead entity. Development of the NCS was technically and financially supported by the Enhancing Cyber Security (ENCYSEC) project[18] that was funded by the EU Instrument contributing to Stability and Peace (IcSP) and implemented by the international technical expertise agency of the French government, Expertise France, and the consulting and service company for the French Ministry of the Interior, Civipol.

The NCS working group convened stakeholders from state institutions as well as representatives from professional associations, the private sector, civil society and international partners. Following initial consultations of the working group, a subset of its members was tasked with preparing a first draft strategy. In October 2015, a concluding workshop of the plenary working group provided opportunity to all involved stakeholders to submit feedback and proposals on the draft strategy and a supporting action plan before the strategy's adoption in January 2016.[19]

Kosovo's NCS and implementing action plan were drafted based on the NCS lifecycle management and key performance indicators developed by the EU Agency for Cybersecurity (ENISA).[20]

Covering the timeframe from 2016 to 2019, the NCS sets forth objectives in five thematic areas: (1) critical information infrastructure (CII) protection; (2) institutional development and capacity building; (3) building public and private partnerships; (4) incident response; and (5) international cooperation.

Specific objectives in these five areas included the identification of CII operators and criteria for their assessment; the creation of a National Cybersecurity Council and the appointment of a National Cybersecurity Coordinator; the organisation of national awareness campaigns and participation in the European Cybersecurity Month; facilitation and participation in national and international cybersecurity exercises; the revision of Kosovo's cybercrime legislation; investments in human capacity building; setting up mechanisms for information exchanges with the private sector; the creation and international accreditation of a national CERT; the participation in international organisations to help promote and implement best practices; and the pursuit of bilateral and multilateral agreements to advance cooperation on cybersecurity matters with like-minded partners.[21]

[18] "ENCYSEC: About," Enhancing Cyber Security, accessed 1 November 2019, https://www.encysec.eu/web/; "Besnik Limaj, Founder and CEO of Logic PLUS and Team Leader of the EU Funded Transregional Project 'Enhancing Cyber Security'," *Cybersecurity Capacity Portal*, 23 March 2015, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/besnik-limaj-founder-and-ceo-logic-plus-and-team-leader-eu-funded-transregional-project.

[19] Ministry of Internal Affairs of the Republic of Kosovo, National Cyber Security Strategy and Action Plan 2016-2019, December 2015, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-national-cyber-security-strategy-and-action-plan-2016-2019.

[20] ENISA, "An evaluation framework for Cyber Security Strategies," November 2014, https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.

[21] National Cyber Security Strategy and Action Plan 2016-2019, 18–22.

Identification of these objectives draws on a general enumeration of risks, possible motivations of threat actors and vulnerabilities in the NCS.[22] These challenges, however, are not contextualised in their applications to Kosovo. Priorities identified on the basis of a generic threat assessment may not be optimised against the particular needs of Kosovo.

The NCS is supported by a detailed action plan that specifies concrete activities for achieving the Strategy's objectives and identifies institutions responsible for implementation, support capacities as well as performance indicators. A number of core activities included in the action plan rely on ENCYSEC assistance, posing obstacles to their planned implementation since the ENCYSEC project was concluded in the same month the NCS was officially adopted.

As envisioned under the NCS, Kosovo has created a National Cybersecurity Council (NCSC) as a coordination platform for stakeholders involved in the implementation of the Strategy. In practice, the NCSC has acted as a vertical reporting vehicle, in the main, and holds no decision-making powers or mandate to take joint action in the event, for instance, of a national-level cyber-incident. The NCSC regularly convenes representatives of the MIA, the Kosovo Police, the Kosovo Forensics Agency, the Ministry of the Kosovo Security Forces, the Kosovo Intelligence Agency, the Agency of the Information Society (AIS), the Kosovo Security Council, the Ministry of Justice, the Kosovo Prosecutorial Council, the Kosovo Judicial Council, the Ministry of Finance, the Kosovo Customs, the Ministry of Education, Science and Technology, the Ministry of Foreign Affairs, the Regulatory Authority of Electronic and Postal Communications (ARKEP), and the Central Bank of Kosovo. Where warranted by the subject of discussion, the NCSC may invite additional ministries or government agencies to participate in a specific meeting. Notably, the default setup does not extend the circle of consultations to the MED.

The NCS further establishes the role of National Cybersecurity Coordinator, who chairs the NCSC and is charged with coordinating, monitoring and reporting on the implementation of the NCS. Under the current NCS, these responsibilities are delegated to the MIA and the role of National Cybersecurity Coordinator is currently fulfilled by the Deputy Minister of Internal Affairs. To assist the National Cybersecurity Coordinator in executing their duties, the NCS has set up a Strategy Secretariat. While the Strategy Secretariat was originally designed to provide further analysis to inform NCSC deliberations, in practice, its work has been described by stakeholders who are familiar with the NCSC's proceedings and who were consulted for this assessment as being focused on administrative support tasks. At the time of this assessment, the MIA had not set up an internal cybersecurity team to support the National Cybersecurity Coordinator and to serve as an expert point of contact within the MIA for other government agencies, to coordinate on cybersecurity initiatives.

Funding to support the implementation of the Strategy is appropriated directly to the agency leading the work on an activity.

NCSC members continuously measure their own progress in the implementation of the NCS and report against the Strategy objectives at Council meetings, which take place at three-month intervals. NCSC meetings tend to focus on collecting statistical evidence to show compliance with performance indicators as identified in the Strategy's action plan. Based on

[22] National Cyber Security Strategy and Action Plan 2016-2019, 10–11, http://www.kryeministri-ks.net/repository/docs/National_Cyber_Security_Strategy_and_Action_Plan_2016-2019_per_publikim_1202.pdf.

participant views, NCSC meetings provided limited opportunity for follow-ups on progress-reporting or discussion about any capacity issues encountered while meeting NCS objectives. Under these circumstances, stakeholders reported reluctance to speak out about shortcomings during NCSC meetings, pointing to a lack of institutional support to address and resolve implementation challenges. In a similar vein, several stakeholders expressed hesitance to raise any identified emerging threats or challenges, as the focus of NCSC meetings on reporting targets offered little opportunity for proactive initiatives to address anticipated difficulties. Based on stakeholder responses, it remains unclear whether all relevant actors have been consistently invited to NCSC meetings by the coordinating body. It was not possible to conclusively assess how–or whether–Kosovo authorities engaged the OSCE on plans for the annual evaluation of progress in the implementation of the NCS as envisioned under the action plan.

According to representatives from several institutions represented on the NCSC, a first internal assessment of the implementation of the NCS and its supporting action plan was conducted in January 2019. This review concluded with a satisfactory evaluation of progress, noting improvements in training, international cooperation, and cooperation between agencies. As a self-assessment based on the reporting of implementing stakeholders to the NCSC, the findings of this review remain to be confirmed by an independent evaluation. Preliminary plans exist for partnering with the OSCE to conduct an external evaluation and organise workshops to discuss learnings from the first implementation cycle. Interviewed implementation stakeholders noted organisational and procedural capacity gains, including a better appreciation of the scope of the challenge involved in operationalising the NCS as part of an inter-agency process. Stakeholders also positively emphasised the value of the communication structures established under the NCS, though the use of these has, so far, mainly been focused on reporting on implementation targets and less on opportunities for coordination and cooperation.

According to stakeholders consulted for this assessment, the MIA is preparing steps to facilitate the development of a follow-up NCS. The Strategic Planning Office within the Prime Minister’s Office has defined the procedure for preparing the next iteration, including a preliminary list of stakeholders to be invited to the process. A planning committee to carry out this work has been set up with the ambition of submitting a new strategy and action plan to the Government by the end of 2019.

Essential conditions for the inclusiveness and substantiveness of the process could not be evaluated at the time of this assessment. Among others, these points included the composition of the planning committee that will lead the drafting efforts for the new NCS; the scope of consultations with additional stakeholders; the key priorities for the successor strategy and the basis for their identification; and any steps taken to coordinate work on the new NCS with the priorities of the planned new iterations of Kosovo‘s *Digital Agenda for Kosova 2013-2020* and *IT Strategy*, to harness synergies and avoid overlaps or blind spots.

In addition to the NCS, two other important planning documents address the implications of technology and inform related policy in Kosovo. The first of these is the *Digital Agenda for Kosova 2013-2020*, which precedes and outlives the first NCS and sets policy for the electronic communication sector. Coordinated by the MED, the *Digital Agenda for Kosova 2013-2020* covers activities across three pillars: (1) development of the ICT infrastructure; (2) development of the electronic content and services and promotion of use thereof; and (3) enhancement of the Kosovar residents' ability to use the ICTs. The document was reviewed in 2016, following adoption of the NCS, and resulted in a shift of the implementation focus towards broadband development.

The main achievements in the implementation of the *Digital Agenda for Kosova 2013-2020* are related to the first pillar. Kosovo is implementing the WBG-funded Kosovo Digital Economy (KODE) project, which aims to improve access to better quality and high-speed broadband services in project areas and to online knowledge sources, services and labour markets among citizens, and public and academic institutions. An emphasis is placed on rural broadband connectivity. KODE became effective in November 2018 and is intended to be active until June 2023.

Efforts associated with the priorities identified in pillar 3 are mainly related to digital skills trainings focused on young people and women. The MED will begin implementation of two projects in 2020, one of which will train approximately 2,000 young people in digital skills within the framework of the KODE project; the other is funded by the EU and will train approximately 1,500 young people through more specific IT courses covering, among others, programming languages and web design. No decision has been made yet about whether cybersecurity courses will become part of these offerings, but the possibility has not been ruled out.

A follow-on *Digital Agenda* will be developed during 2020, drawing on input from ARKEP, along with stakeholders from other government institutions and the private sector. As far as cybersecurity aspects are concerned, this new *Digital Agenda* is expected to focus on issues related to the security and integrity of electronic communications networks and services, as well as measures to increase public and business confidence in the safety of cyberspace.

The second planning document concerning technology policy is Kosovo's *IT Strategy*. Developed by the MED with support from Germany's development agency, GIZ, and the Norwegian Embassy, and in cooperation with the private-sector Association for Information Technology and Communication of Kosovo (STIKK), the *IT Strategy* is focused on developing Kosovo`s domestic IT industry as well as exports of Kosovar IT products and services abroad. As such, the *IT Strategy* includes measures that seek to enhance the quality and security of software and services. To this end, it supports education and training of talent as well as the adoption of international best practices and recognised technical standards. Adopted in June 2016,[23] the initial *Strategy* reached its implementation cycle at the end of 2018. A review of the *IT Strategy* is planned for 2020, in cooperation with private and public sector stakeholders and will include an assessment of the implementation of the previous strategy.

[23] "Information Technology Strategy – A Step Towards Digital Economy," Ministry of Economic Development of the Republic of Kosovo, 27 June 2016, https://www.mzhe-ks.net/en/news/information-technology-strategy---a-step-towards-digital-economy.

D1.1 National Cybersecurity Strategy		
Areas of Capacity Advancements	**Areas of Consolidation**	**Enduring Challenges**
↑ Development of National Cybersecurity Strategy (NCS) informed by broad stakeholder consultations ↑ Adoption of NCS and detailed action plan ↑ Completion of first implementation cycle and monitoring of performance based on action plan indicators ↑ Creation of inter-agency support structures (National Cybersecurity Council and National Cybersecurity Coordinator) to streamline implantation and progress reporting	→ Coordination of parallel strategic initiatives (NCS, Digital Agenda and IT Strategy) with regard to their respective responsibilities for cybersecurity	! Leveraging NCS support structures to identify and address implementation challenges ! Independent evaluation of NCS implementation, including the identification of lessons learnt that can feed into the development of a follow-on NCS
Maturity Levels in Comparison 2015 : 2019		
2015 – Start-up	2019 – Formative to Established	

D 1.2 INCIDENT RESPONSE

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

Stage: Formative

KOS-CERT, Kosovo's national cyber-incident response unit, took up operations in July 2016. KOS-CERT is structurally integrated into the telecom regulator ARKEP, which oversees network and electronic service providers. With its basis in the *Law on Electronic Communications* (Art.10.21),[24] KOS-CERT is tasked with technical incident response and raising awareness but it has no explicit mandate defining responsibilities and duties. KOS-CERT structures and procedures are based on the original model implemented by Lithuania (prior to its reorganisation in 2017) that had set up a national incident response capacity under the

[24] Law on Electronic Communications of 2012, no. 04/L-109, Official Gazette of the Republic of Kosovo 30/2012, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2851.

Communications Regulatory Authority of Lithuania. Following this approach, KOS-CERT was set up under ARKEP.

At the time of this assessment, KOS-CERT faced a severe personnel shortage and was only operated by two staff. In the absence of an official mandate, and with limited human capacity to develop procedures of its own, the response team at KOS-CERT has turned to the practices of Lithuania's CERT for guidance. KOS-CERT has sought to strengthen coordination among organisational incident response teams both within the private and public sector, to facilitate and expand information sharing. These efforts have been constrained by low response rates from contacted organisations, though good cooperation exists with Internet service providers (ISPs) and mobile providers that operate under the regulatory auspices of ARKEP. While KOS-CERT has no formal agreement with the Cybercrime Investigations Unit of the Kosovo Police, the team will share technical information with the unit on an *ad-hoc* basis.

The unit receives a relatively low number of direct incident reports, which the team attributes to insufficient capacities of institutions to detect incidents. As an institution accredited with Trusted Introducer, KOS-CERT uses the service's taxonomy of incidents to categorise detections and reports. KOS-CERT provides an incident reporting form on its website[25] and users and organisations can also submit incident reports by telephone and email. Submissions are registered through a Request Tracker for Incident Response (RTIR) ticketing system. The system currently operates without automated incident classification, which needs to be introduced manually. A vulnerability bulletin is published weekly on the KOS-CERT website.

Kosovo has not yet received a country-code top level domain (TLD) from the Internet Assigned Numbers Authority (IANA); country-code TLDs are commonly only delegated on the basis of country codes recognised in ISO 3166,[26] which in turn is based on a country's membership in the United Nations.[27] The lack of a country-code TLD has limited Kosovo's integration into a regional Internet registry and results in Internet protocol (IP) addresses for devices physically located in Kosovo being listed as registered in Albania or Serbia. These misattributions mean that incident reports from international partners concerning IP addresses in Kosovo are likely to be directed to Albania or Serbia instead of to the administering ISPs in Kosovo. In the past, Albania has generally forwarded incident reports and cooperation with Serbia is achieved on a case-by-case basis. Dependence in this vein on external collaboration, however, has slowed down the receipt of time-sensitive information.

Around 50 incident-response teams operate across Kosovo, including ministries, government agencies and private sector organisations—such as major banks and ISPs—with select ISPs running or setting up three-tier security operations centres (SOCs). Levels of competency and capacity vary significantly among these units, with only a small proportion being able to independently detect incidents. Distributing and replicating incident-response capacities across ministries and Government has increased sunk costs and left advantages of economies of scale untapped at a time when the national CERT is understaffed. A significant number of institutional response teams within Government face similar shortages of cybersecurity

[25] Incident Reporting Form, KOS-CERT, accessed 1 November 2019, https://kos-cert.org/index.php/raporto_incident_en.
[26] IANA, "Domain Name System Structure and Delegation," RFC 1591, March 1994, https://tools.ietf.org/html/rfc1591.
[27] "ISO 3166 Country Codes," International Organization of Standardization, accessed 1 November 2019, https://www.iso.org/iso-3166-country-codes.html.

expertise. Many of these in-house units were not supported by new hires when they were set up. Instead, these response teams were formally assigned civil servants who, nonetheless, continue to carry out the full-time duties that they had held before, at times resulting in what the local community has described as “fictional CERTs”, referring to institutional structures without actual operational capacity.

The University for Business and Technology (UBT) in Pristina has established a CERT for the academic community. UBT-CERT[28] evolved out of a project focused on standards for cybersecurity and privacy that has developed a network across industry, academia and civil society. At the moment, UBT-CERT offers its incident response services to public and private-sector organisations, together with cybersecurity trainings and penetration-testing services.

No general incident reporting requirements exist by law in Kosovo. Provisions within the 2012 *Law on Electronic Communications* have allowed ARKEP to set requirements for electronic communication network and service providers to report to it any breach of security or loss of integrity that is expected to have a significant impact on the continued operations of their networks or services (Art.85.5). In 2016, ARKEP issued the corresponding regulations[29] that give full force to this provision and specify the criteria for the impact assessment to be conducted by the operator and submitted to ARKEP. Based on the same regulation, ARKEP has the authority to impose sanctions on operators (Art.11), including in cases where operators have failed to implement adequate technical or organisational measures to preserve the integrity of public networks, failed to notify ARKEP of security incidents, or failed to do so within the prescribed timeframe, as well as in cases where operators have conducted a non-genuine impact assessment of the incident or provided an inaccurate characterisation of its effects.

Operators of other sectors that are likely to be designated as critical national infrastructure (CNI) when new sub-legal acts on CNI identification are passed reported a low use of Internet-based technology and systems. For the event of failing industrial control systems, operators consulted for this assessment reported the existence of mechanical backup operations or possibilities of manual resets designed to ensure continued delivery of service. Cybersecurity measures and related awareness were perceived as subordinate concerns and operators generally not trained in these matters. Where a specific need for technical expertise arises, operators hire contractors with the necessary qualifications, though cybersecurity budgets to respond to any contingency appear to be minimal. Training on cybersecurity, if pursued by operators, is commonly based on their own interest and initiative.

[28] “UBT-CERT Mission,” University for Business and Technology, accessed 1 November 2019, https://csp.ubt-uni.net/cert/en/.

[29] ARKEP, Regulation on Technical and Organisational Standards for Security and Integrity of Electronic Communication Networks and/or Services of 2016*,* Prot. No. 046/B/16.

D1.2 Incident Response		
Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ National computer incident response team formally established (KOS-CERT) ↑ Limited sectoral requirements on incident reporting	→ Designation of critical infrastructure and expansion of sectoral cybersecurity requirements	! KOS-CERT operates with minimal staff and resources ! Incident response capacities are distributed across ministries and agencies ! Institutional CERTs (within government) lack operational capacity

Maturity Levels in Comparison 2015 : 2019

2015 – Start-up | 2019 – Formative

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

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

Stage: Start-up

In 2018, Kosovo adopted the *Law on Critical Infrastructure*[30] based on EU Council Directive 2008/114/EC on the identification and designation of critical infrastructure. The law was developed under the leadership of the MIA and entered into force in April 2019. As umbrella legislation, the law relies on sub-legal acts for implementation and only provides for procedures for the identification and designation of CNI operators. On its own, the law does not contain any provisions specific to CII. The law tasks the MIA with the development of a sub-legal act by the end of July 2019 that is to establish a National Critical Infrastructure Policy and to provide further guidance on critical infrastructure protection and facilitate the sharing of critical infrastructure protection information (Art.4.2).

The MIA is leading the process for identifying CNI under the law, in consultation and cooperation with security institutions, Government and non-Government institutions, public and private owners and operators of potential CNI systems and relevant international stakeholders (Art.6.1).

[30] Law on Critical Infrastructure of 2018, no. 06/L-014, Official Gazette of the Republic of Kosovo 5/2018, https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313.

Identification procedures are to be conducted following a comprehensive risk analysis that evaluates the potential disruption or destruction of critical infrastructure in its impact on the economy, society and political stability (Art.6.2). This comprehensive risk analysis is to assess impact based on a series of cross-cutting and sectoral criteria, including geographic distribution, economic, political, psychological, environmental impact and effects on public health under the consideration of relevant dependencies and interdependencies (Art.6.3). These criteria are to be finalised six months from the date that the law came into force, i.e. by the end of October 2019. Only then can the risk assessment be conducted, and only with the risk assessment can CNI operators be identified and designated, concluding a lengthy procedure that significantly deviates from the timeline written into the NCS action plan that had anticipated the adoption of a law on CNI protection for the end of 2016.

Close coordination between the MIA and the MED forms a crucial condition for the identification of CNI operators, as the MED oversees Government management of publicly-owned enterprises,[31] a range of which are likely to qualify for CNI designation.

Kosovo is undertaking a two-track effort to transpose the EU Network and Information Security (NIS) Directive based on a concept study conducted in 2018 that was approved by the Government in June 2019. Select elements of the NIS Directive have been integrated into the new comprehensive cybersecurity law that is being drafted by the MIA. The MED has reviewed relevant provisions of the new draft cybersecurity law and is preparing complementary legislation to ensure the complete transposition of the NIS Directive with close regard to avoiding any duplication of efforts. The MED is planning to set up a working group in early 2020 to prepare a draft law for transposing the NIS Directive based on input from all public- and private-sector institutions concerned within the scope of the law. Preliminary consultations in 2018 for the concept document, among others, had convened representatives from the energy, transport, banking, health and financial sectors, as well as drinking-water-supply and water-distribution companies. Following public consultation, the law is scheduled to be submitted to Parliament for approval by the end of 2020.

In addition to incident reporting and impact assessment requirements described above (see section D1.2 of this report on Incident Response), ARKEP has also introduced security audit requirements for electronic communication network and service providers under its supervision based on the *Law on Electronic Communications* (Art.85.4), which also regulates the imposition of possible sanctions (Art.101-103). Independent audits are to be conducted and paid for by providers reporting revenue in the excess of €500,000, to demonstrate compliance with the technical and organisational standards specified by ARKEP in 2016 based on ENISA guidelines.[32]

At the time of reporting, four ISPs controlling 80 percent of Kosovo‘s market have completed their first audit. Aggregated auditing results are presented on a scale from 0 to 4 (where 0 = not implemented and 4 = fully implemented). Assessed ISPs mostly obtained scores between

[31] “Scope of the Ministry of Economic Development,” Ministry of Economic Development of the Republic of Kosovo, 1 November 2019, https://mzhe-ks.net/en/scope-of-the-ministry-of-economic-development.

[32] ARKEP, Regulation on Technical and Organisational Standards for Security and Integrity of Electronic Communication Networks and/or Services, Prot. No. 046/B/16, Art.8.

2.5 and 3. Re-evaluations are scheduled every two years, to assess how audit recommendations have been implemented.

Management of Kosovo's electricity grid relies on a centralised Supervisory Control and Data Acquisition System (SCADA). The *Energy Strategy of the Republic of Kosovo 2017-2026* foresees the integration of sub-stations into this central SCADA system.[33] The strategy includes no references to cybersecurity concerns or measures for protection to ensure the resilience of expanded SCADA operations.

Kosovo's largest water company runs two SCADA systems at two separate facilities that have been set up by Bulgarian contractors. Maintenance of these systems is also outsourced to contractors abroad. Network administrators and engineers on site had only minimal contact with these contractors, and no training to manage the response to a security incident in-house.

Most major financial institutions operating in Kosovo are subsidiaries of international firms that follow guidelines established by their headquarters outside of Kosovo, including processes based on ISO 27001. Yet, no specific local requirements exist that make their implementation compulsory. The Central Bank is preparing the introduction of specific IT requirements for financial institutions as part of the Regulation on Information Technology for Banks that is currently under development.

D1.3 Critical Infrastructure (CI) Protection		
Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ Adoption of framework legislation for the designation of CI	→ Comprehensive cross-cutting risk assessment foreseen under CI law	! With the exception of ISPs, no specific ICT security requirements for *de facto* CNI operators ! Planned expansion of SCADA operations for electric grid lacks strategic consideration of cybersecurity concerns ! Limited on-site incident response expertise for critical operators

Maturity Levels in Comparison 2015 : 2019

2015 – Start-up	2019 – Start-up

[33] Ministry of Economic Development of the Republic of Kosovo, Energy Strategy of the Republic of Kosovo 2017-2026, March 2017, 10–11, https://mzhe-ks.net/repository/docs/Kosovo_Energy_Strategy_2017_-_26.pdf.

D 1.4 CRISIS MANAGEMENT

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

Stage: Start-up

The NCSC, Kosovo's main coordinating body for cybersecurity policy, presently holds no mandate to prepare or coordinate joint action to manage the response to a national-level crisis.

The 2011 *Law for Protection against Natural and Other Disasters*,[34] in its definition of "other disasters", includes specific mention of extraordinary emergency situations involving telecommunications and IT (Art.3.1.6). The law designates the Emergency Management Agency (EMA) under the MIA as the responsible body for developing a national disaster recovery plan (Art.94). This plan has still to be tested in the scenario of a national-level cyber-incident. To what extent training programmes provided by EMA's Integrated Training Centre (Art.110-111) specifically prepare for incidents affecting information systems and technology could not be ascertained within the scope of the consultations for this assessment.

NCS objectives included the development of a national programme to test and evaluate existing incident response capacities in cybersecurity exercises.[35] The action plan supporting the implementation of this programme sought to enlist assistance from ENCYSEC for the design of test scenarios and cybersecurity exercises. As mentioned above, ENCYSEC, however, concluded its operations at the time of the action plan's adoption and before implementation of any activity could be undertaken.

Institutional capacities have been tested in individual national and international exercises. In 2017, KOS-CERT participated in the International Telecommunication Union's (ITU) Regional Cyberdrill for Europe and CIS Regions,[36] which facilitated a side meeting between the incident response teams of the Western Balkan Six (Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia) to discuss cybersecurity issues in their implications on the economy, the threat landscape in the Western Balkans, and potential for cooperation among the six parties.[37]

The 2018 edition of the Silver Sabre Exercise conducted by KFOR, the NATO-led peacekeeping force deployed in Kosovo, contained elements for the test of emergency-response assets in the face of a cyber-incident. The exercise was conducted with participation from the EU Rule

[34] Law for Protection against Natural and Other Disasters of 2011, no. 04/L-027, Official Gazette of the Republic of Kosovo 22/2011, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2775.
[35] National Cyber Security Strategy and Action Plan 2016-2019, 20.
[36] "ITU Joint ALERT cyber drill for Europe and CIS Regions," ITU, accessed 1 November 2019, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Moldova_cyberdrill_2017.aspx.
[37] "RCC: Chisinau Hosts Cyber Security Drill for Europe and CIS Regions," Regional Cooperation Council, 21 November 2018, https://www.rcc.int/news/323/rcc-chisinau-hosts-cyber-security-drill-for-europe-and-cis-regions.

of Law Mission in Kosovo (EULEX), the Kosovo Security Council (KSC), the Kosovo Police (KP), the Kosovo Security Forces (KSF) and EMA.

In cooperation with the Iowa National Guard, the KSF organises the Eagle exercise series on an annual basis in Kosovo. The exercise is regularly joined by neighbouring countries and other European partners. For the seventh edition in 2020, the KSF plans to introduce a cyber-component to the exercise for the first time.

On occasion, Kosovo's diplomatic status has affected opportunities to participate in exercises organised by international organisations belonging to countries that do not officially recognise Kosovo.

D1.4 Crisis Management		
Areas of Capacity Advancements	**Areas of Consolidation**	**Enduring Challenges**
↑ Test of institutional capacities and inter-agency coordination in national and regional exercises with limited cyber-components	→ National disaster recovery plan exists but has yet to be tested against a national-level cyber-incident	! National Cybersecurity Council not integrated into national-level crisis response

Maturity Levels in Comparison 2015 : 2019

2015 – Start-up	2019 – Start-up

D 1.5 CYBER DEFENCE

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

Stage: Start-up

Kosovo is ranked number 23 in terms of countries with the lowest military expenditure.[38] The Kosovo Security Force (KSF) comprises an active-duty component of 2,500,[39] though new legislation has raised the ceiling of active personnel to twice the size of the current force and

[38] https://data.worldbank.org/indicator/MS.MIL.XPND.CD?most_recent_value_desc=false

[39] "Military expenditure (current USD)," World Bank, accessed 1 November 2019, https://www.globalsecurity.org/military/world/europe/ks-ksf.htm.

envisions a reserve component of up to 3,000 members.[40] Capacity challenges of the KSF generally, related to limited resources and personnel, also translate to its cybersecurity efforts.

While the KSF set up a CERT already in 2015–before KOS-CERT became operational–the team is presently composed of only a single member after rotation in assignments recently reduced the headcount from three. Plans made by KSF include raising this number to 15 but that will likely run into recruitment difficulties or will require investment in additional time to train up qualified personnel.

CERT-KSF-RKS reports to the Minister of Defence as the director of the CERT and is officially tasked with managing cyber-incidents to provide mission assurance in protecting information systems and services of the KSF. In its current composition, the team is unlikely to be in a position to fulfil this mandate if faced with a serious incident. CERT-KSF-RKS is listed with Trusted Introducer.[41]

Plans for a new comprehensive cybersecurity legislation (for additional details, see section D4.1 of this report on Legal Frameworks) reportedly will exclude the defence sector from consideration.

D1.5 Cyber Defence

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ Military incident response capacity formally set up, focused on mission assurances and protecting KSF systems and services		! CERT-KSF-RKS lacks staff and resources to fulfil its mandate

Maturity Levels in Comparison 2015 : 2019

2015 – Start-up	2019 – Start-up

[40] Law on the Kosovo Security Force of 2019, no. 06/L-123, Art.23.3, Official Gazette of the Republic of Kosovo 1/2019, https://gzk.rks-gov.net/ActDetail.aspx?ActID=18375.
[41] "CERT-KSF-RKS," Trusted Introducer, accessed 1 November 2019, https://www.trusted-introducer.org/directory/teams/cert-ksf-rks.html.

D 1.6 COMMUNICATIONS REDUNDANCY

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

Stage: Formative

Under provisions of the *Law on Electronic Communications* (Art.75, 105), electronic communications network and service providers are obliged to make their networks and services available to support Government communication efforts in extraordinary emergency situations. Providers are required to develop and submit to a plan to ARKEP, detailing measures to ensure the integrity and continued availability of public communication networks in the event of serious network damages, natural disasters or emergencies in a state of war. Measures undertaken under this plan need, in particular, to ensure the uninterrupted access and use of emergency numbers.

The *Law for Protection against Natural and other Disasters* also delegates responsibilities for a range of preparatory measures to ensure the continued operation of electronic communication tools in emergency situations affecting communication infrastructure. Within their respective remits, central and local government authorities are responsible for building and maintaining electronic communication capacities as part of a dedicated communication system that enables emergency and rescue services to continue their work in the event of a wider collapse of communication networks (Art.36.1.9, Art.37.2.3). Central authorities are required to ensure their continued ability to communicate with local level authorities. To facilitate rescue and emergency assistance efforts and carry out wider crisis management responsibilities, the MIA in its coordinating role in disaster management is required to set up an autonomous system of electronic communication (Art.53.2).

Individual government agencies have response units equipped with microwave antennas to bridge over local ruptures in connectivity.

Banks and insurance companies, based on industry regulations for business continuity, need to maintain parallel subscriptions with at least two ISPs and to operate data recovery centres. These companies, however, do not regularly evaluate whether contracted ISPs rely on the same upstream connection.

D1.6 Communications Redundancy (*referred to as "Digital Redundancy" in CMM Report Kosovo 2015*)

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
	→ Central authorities are responsible for ensuring communication with local authorities and can draw on commercial communication providers → MIA is mandated to establish autonomous communication system → ISPs are required to develop redundancy measures for their networks → Financial institutions are obliged to maintain parallel subscriptions with at least two ISPs → Individual agencies maintain capacities to address local connectivity issues	! All redundancy requirements and emergency communication systems, as established by law, require regular testing

Maturity Levels in Comparison 2015 : 2019

2015 – Formative	2019 – Formative

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the GCSCC has developed the following set of recommendations for consideration by the Government of Kosovo. These recommendations provide advice and steps aimed at increasing existing cybersecurity capacity as per the considerations of the Centre's CMM. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 Conduct an independent evaluation of the NCS 2016–2019; draw on the learnings from this assessment for the development of any follow-on NCS.

R1.2 Ensure close coordination between the MIA and MED as central actors in strategic planning initiatives and legislation related to cybersecurity, to harness synergies and to avoid any duplication of efforts and blind spots.

R1.3 Review membership of the NCSC and ensure that all relevant institutions are represented as permanent member in NCSC meetings.

R1.4 Use NCSC meetings as an opportunity to address and devise solutions for implementation challenges; structure NCSC meetings to allow for opportunities to proactively address anticipated challenges or capacity issues that may limit a stakeholder's ability to deliver on agreed objectives.

R1.5 Strengthen the Strategy Secretariat to provide substantial support and assist with the resolution of any capacity issues discussed during NSCS meetings, based on the advice of the National Cybersecurity Coordinator.

R1.6 To strengthen implementation capacity, consider adapting the approach followed in setting up Kosovo's National Security Council; invite subject matter experts from partner governments to shadow local officials and provide guidance and pass on best practices.

R1.7 Create a point of contact with cybersecurity policy expertise within the MIA to serve as liaison for coordination with other government agencies on cybersecurity initiatives.

R1.8 Conduct a rigorous cybersecurity risk assessment specific to the conditions of Kosovo to inform the focus of a follow-on NCS.

R1.9 Ensure repeated rounds of inclusive and substantive consultations that convene all relevant national stakeholders and international partners to inform any follow-on NCS.

R1.10 Provide for appropriate budgetary support to ensure the full implementation of any follow-on NCS. Financial resources might be allocated as part of a centralised budget dedicated to NCS implementation or earmarked for specific implementation activities directed to the various implementers identified in the action plan.

R1.11 Establish rigorous but realistic metrics to monitor implementation of any follow-on NCS.

INCIDENT RESPONSE

R1.12 Provide KOS-CERT with a clear mandate, specifying roles and responsibilities.

R1.13 Support KOS-CERT with an appropriate staff count for the team to fulfil its responsibilities.

R1.14 Provide KOS-CERT with the necessary resources for analysts to undergo regular training.

R1.15 Ensure incident response teams within government agencies are supported with the resources and staff available to carry out their responsibilities; consider the creation of an overarching government CERT to provide reliable service to government agencies at scale (for instance, through the further development of existing capacities within the Ministry of Public Administration).

R1.16 Expand incident-reporting requirements to other sectors in line with upcoming legislation on the identification and designation of critical national infrastructure systems and their operators.

R1.17 Establish mechanisms for institutionalised information sharing between the public and private sector.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.18 Ensure the timely preparation of the necessary sub-legal acts to give full force to the *Law on Critical Infrastructure* and facilitate the identification of CNI operators and CII systems.

R1.19 Make cybersecurity requirements an integral component of regulations to strengthen the resilience of designated CNI operators and associated CII systems; consult with ARKEP on lessons learned from implementing initial requirements for the electronic communications sector.

R1.20 Ensure close coordination between the MIA and MED in the assessment of publicly-owned enterprises under the supervision of the MED as part of the CNI identification process.

R1.21 Establish mechanisms for the exchange of threat and vulnerability information among CNI owners as well as between CNI and the government.

R1.22 Coordinate responsibilities in the transposition of NIS Directive to avoid any overlaps between the dedicated law for transposing the NIS Directive and efforts led by the MIA in the implementation of the *Law on Critical Infrastructure*.

CRISIS MANAGEMENT

R1.23 Consider expanding the mandate of the NCSC to prepare and coordinate the response to national emergencies as they relate to cyber-incidents and elevate the NCSC as a platform for collective crisis response for cyber-incidents.

R1.24 Implement the NCS plans to develop a programme for cybersecurity exercises that test and facilitate improvements of incident response mechanisms.

R1.25 In support of the cybersecurity exercise programme, specify the parameters and capabilities that are to be tested. Ensure that national disaster recovery and crisis management plans coordinated by EMA account for scenarios of a national-level cyber-incident and failures of critical information systems.

R1.26 Ensure that EMA training programs prepare for incidents affecting information systems.

CYBER DEFENCE

R1.27 Ensure the appropriate staffing of CERT-KSF-RKS so that the team can deliver reliably on its responsibility of mission assurance.

R1.28 Explore options for setting up a cyber-reserve that allows technical experts from the private sector to serve in the KSF for short deployments or on a needs basis.

COMMUNICATIONS REDUNDANCY

R1.29 Ensure that emergency communications and backup systems are in place, as required by law.

R1.30 Conduct regular testing of dedicated emergency communication systems, including inter-operability tests between central and local authorities.

R1.31 Evaluate existing backup communication systems for gaps and overlaps in communication links.

DIMENSION 2
CYBER CULTURE AND SOCIETY

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

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

D 2.1 CYBERSECURITY MIND-SET

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

Stage: Formative

The consulted stakeholders described a *formative* stage of a cybersecurity mind-set in Kosovar society. Some parts of the private sector, users, and the Government have begun to prioritise cybersecurity by identifying risks and threats, but this process requires time to extend cybersecurity good practices to the majority of society. Regular Internet users are concerned with cybersecurity but in an *ad-hoc* manner, often after a negative experience online or when making transactions involving bank details. Although Internet penetration is extended over Kosovar society, especially on a household level,[42] there are initiatives to improve Internet access to all its settlements as the objective of the KODE.[43] Only a limited proportion of users (younger generations) have a more advanced and proactive cybersecurity mind-set.

The Government of Kosovo has some internal cybersecurity practices established as a requirement, such as using internal networks to secure communication between public agencies or conducting a penetration test before publishing any governmental website (with the test conducted by the AIS). These practices increase the cybersecurity awareness of a proportion of civil servants but, in general, there is not a routinised cybersecurity mind-set.

In the private sector, some leading firms place priority on cybersecurity, identifying high-risk practices and introducing good practices to reduce such risks. This is particularly the case within large institutions, firms in the ICT sector, firms in the banking sector, and international firms. International firms in particular usually have their own protocols and programmes to harmonise cybersecurity practices across their different divisions in different countries, encouraging a healthy cybersecurity environment inside the company, with their employees, and externally, with their clients and providers. However, these practices are not typical of the rest of the private sector.

The consulted participants observed a generational gap in ICT skills and cybersecurity awareness, with younger generations of Internet users being better informed than older users about the importance of cybersecurity. As managers in responsible positions are usually employed by more experienced workers, if no other training takes place, it would take time to substitute older generations of managers with younger ones who could develop a cybersecurity mind-set throughout the whole private sector. Generations do not determine one's mind-set, however, so more training is essential to build cybersecurity good practices at management level. In addition, those participants in sectors that do not use ICT in their daily activities show less concern regarding cybersecurity; so long as the sector does not adopt these technologies, they feel cybersecurity is not a priority.

Overall, since 2015, Kosovar society has consolidated its *formative* maturity stage in the cybersecurity mind-set. Four years ago, the indicators of this factor described a cybersecurity mind-set close to a *formative* maturity stage but the consultations with stakeholders were dubious, particularly regarding the cybersecurity mind-set of the Government. Today, Kosovo is in a *formative* maturity stage in all its indicators and actors, including the Government, and society as a whole appears to be taking steps towards extending good cybersecurity practices to the majority if its members, moving towards a more *established* stage for a cybersecurity mind-set in the near future.

[42] "Përmbledhje e Indikatorëve Kryesorë të Komunikimeve Elektronike *Pasqyrë e Tregut të Komunikimeve Elektronike* për TM2 2019", ARKEP, accessed 15 November 2019, http://arkep-rks.org/repository/docs/Pasqyra%20e%20tregut%20t%C3%AB%20KE%20_Indikator%C3%ABt%20kryesor%20p%C3%ABr%20%202019%20TM%202.pdf.

[43] "Kosovo Digital Economy (KODE)", World Bank, accessed 15 September 2019, http://projects.worldbank.org/P164188/?lang=en&tab=overview.

2.1 Cybersecurity Mind-Set

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
	→ Growing proportion of Kosovar society that prioritises cybersecurity	! Persistent gap in the cybersecurity awareness of older and younger generations

Maturity Levels in Comparison 2015 : 2019

2015 – Formative	2019 – Formative

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

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

Stage: Formative to Established

After consultations with stakeholders, most Internet users see Internet and online services simply as a means to conduct the services it can facilitate, not how it does so. Only a limited proportion of Internet users possess the ability to protect themselves online and ensure their secure use of the Internet. Similarly, very few operators of the Internet's infrastructure develop measures to promote trust in online services and if they do, these measures have not been established as programmes. The participants' impression is that Internet service providers (ISPs) work correctly but that they do not filter malicious Internet traffic. Regarding practices of processing personal data, there are user-consent policies in place, because personal data may only be processed under the consent of the data subject by law.[44]

The Government of Kosovo provides some e-services through an online portal, mostly devoted to processing tax payments (Kosovo Tax Administration). This portal uses secure login and payment methods which, at the same time, rely on the secure systems of banks for fulfilling the security of the payment. Stakeholders in the private sector emphasised that the vast majority of businesses are using e-government services for paying taxes because of its efficiency. At the same time, they claimed that although the Government is investing in digitalising its services, there should be a proportional investment in security measures.

[44] Law No. 03/L-172 of 2010 on the Protection of Personal Data, Chapter III, https://www.afapdp.org/wp-content/uploads/2012/01/Law-on-Personal-Data-Protection-Kosovo.pdf.

The need for security in e-government services is recognised as well by the Government, and there is an ongoing public procurement process to contract services of authentication modules to monitor the security of each transaction in the portal and strengthen the protection of the users' anonymity. The Government of Kosovo and public agencies offer other e-government services, such as an e-procurement system, and plan to increase their provision. This is considered at the internal level as well; for example, the Ministry of Public Administration has a strategy of modernisation (2015–20) that includes a broad digitalisation of administrative processes,[45] and the AIS aims to ensure the implementation of an e-governance strategy in Kosovo.[46]

Regarding e-commerce services, few companies are active in this sector and users are concerned about the security of transactions involving their personal bank account information. In 2017, while 15.1 percent of Kosovar population over 15 years old used the Internet to pay bills or to buy something online in the past year, the percentage of 15-year-olds in the Euro area or OECD countries was over 68 percent.[47]

Gjirafa is the main company providing e-commerce services in Kosovo and is fully established in the Balkans. This company has promoted the use of e-commerce in Kosovo by providing a good service not only online, but also over the telephone. As a result, a growing proportion of users trust in the secure use of e-commerce services and Gjirafa is helping to educate masses on cybersecurity when buying online. After consultations with stakeholders of the private sector and the Government, it seems the reform of *Law No.04/L-155 on Payment Systems* will encourage firms to adopt e-commerce services.

Compared to 2015, trust and confidence on Internet in Kosovo has consolidated its *formative* maturity stage and is signalling some indicators of an *established* maturity stage. The major advancements have been done in e-commerce and e-government services. To illustrate this change, the available data regarding the percentage of population over 15 years old who used the Internet to pay bills or to buy something online in the past year shows an increase from 5.2 percent in 2014 to the mentioned 15.1 percent in 2017.[48]

[45] "Strategy on modernization of public administration 2015-2020", Ministry of Public Administration, accessed 15 October 2019, https://map.rks-gov.net/desk/inc/media/45EC87EE-FEE9-4F50-86C2-A8EB252162C7.doc.

[46] "AIS", Ministry of Public Administration, accessed 15 October 2019, https://map.rks-gov.net/page.aspx?id=2,14.

[47] "Global Financial Inclusion", World Bank, accessed 15 October 2019, https://databank.worldbank.org.

[48] "Global Financial Inclusion", World Bank, accessed 15 October 2019, https://databank.worldbank.org.

D2.2 Trust and Confidence on the Internet		
Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ Stakeholders recognise the need for security in e-government services ↑ Growing proportion of users' trust in using e-government and e-commerce services		! No evidence ISPs established programmes to promote trust and confidence in online services

Maturity Levels in Comparison 2015 : 2019

2015 – Formative	2019 – Formative to Established

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

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

Stage: Formative

The perceptions of stakeholders reflect that users have minimal knowledge of how personal information is handled online. There is evidence of a debate about the protection of personal information in the public sector. The National Agency for Protection of Personal Data (NAPPD) is an independent agency, managed by a Council consisting of the Chief State Supervisor and four National Supervisors for a mandate of five years, which supervises the implementation of rules and laws regarding personal data protection. Other responsibilities of the NAPPD are the promotion of public awareness on rights and fundamental freedoms on personal data and privacy, and provision of advice to public and private institutions on the balance between the right of protection of personal data and the right to access public documents. However, as explained in its annual report,[49] NAPPD does not have enough human resources to achieve the planned objectives of the agency or the necessary funds for implementing all the campaigns necessary for raising awareness.

Factor *D2.3 User Understanding of Personal Information Protection Online* was not incorporated in the 2015 CMM review, as it was added by the GCSCC at a later date. However, there are some signals that citizens of Kosovo are more aware of personal information protection online than four years ago. NAPPD registered several metrics that can be helpful in

[49] "Annual Work Report 2018", APPD, accessed 15 September 2019, http://www.amdp-rks.org/repository/docs/ENG___Raporti_Vjetor_i_Pun__s_p__r_2018_2232019.pdf.

this sense and are included in its 2018 annual report. First, there has been an increment of the number of responses provided to questions raised by the media, civil society, controllers, and citizens (from 29 responses given in 2012 to 87 in 2018, with a large jump from 2017 to 2018 – 45 additional responses – mainly driven by the new law on data protection).

Regarding the evolution of citizens' complaints on personal data protection, there was an increase of complaints from 2012 (16 complaints) to 2015 (131 complaints), followed by a reduction of complaints until 2018 (42 complaints). In its 2018 report, NAPPD interprets this development as an increase in citizens' knowledge of their rights. However, the recent reduction of number of complaints can be caused by other determinants as well. NAPPD should make sure that the mechanisms in place are designed to deal with any complaint regarding personal information protection.

D 2.4 REPORTING MECHANISMS

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

Stage: Formative

Several channels exist to report cyber-enabled incidents, the main channel being the KP's online platform.[50] Regarding child abuse and cyber bulling, there is no specific channel for reports. There are organisations in the civil society sector (Centre for Advanced Studies FIT, Forumi i Iniciatives Qytetare FIQ, Kosovo Education Centre, etc.) that intervene to prevent school violence, and the Directors of pre-university educational institutions are responsible for reporting any case of violence (including cyber bulling) to the police. Complaints about any irregularity in the processing of personal data can be sent to NAPPD, either online or manually.[51] The National Cybersecurity Unit KOS-CERT also has an online channel to report incidents.[52] However, it seems users are not aware of the existing reporting mechanisms.

During the consultations with stakeholders, participants explained that cyber victims usually do not use the reporting mechanisms mentioned above. They go to the closest police office, where they are directed to the cybercrime police (the Investigation Department in Kosovo Police cooperates with the Division against the Organised Crime on cybercrime). In cases involving a particular social media platform, victims usually report directly to the platform.

[50] "Report Cybercrime", KP, accessed 15 October 2019, http://www.kosovopolice.com/en/report-cybercrime.
[51] "Complaints", APPD, accessed 15 October 2019, http://www.amdp-rks.org/?page=2,6#.XadDKehKguW.
[52] "Report Incident", KOS-CERT, accessed 15 October 2019, https://kos-cert.org/index.php/raporto_incident_en.

Overall, there is a need to better promote the use of the existing reporting mechanisms among Kosovar citizens.

D 2.5 MEDIA AND SOCIAL MEDIA

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

Stage: Start-up

The perceptions of stakeholders are that cybersecurity issues are rarely covered in the media or on social media. Most of the consumers of social media tend to use these platforms to contact family and friends in the country and, because of the Kosovo diaspora, abroad. Organisations with initiatives in cybersecurity use social media and media to disseminate and promote their activities. However, the discussion of cybersecurity is very limited, and participants highlighted the need to raise cybersecurity awareness in the media industry.

RECOMMENDATIONS

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

CYBERSECURITY MIND-SET

R2.1 Make cross-sector cooperation and information-sharing among private and public sector organisations routine, with initiatives on cybersecurity (universities, NGOs, KP, NAPPD, etc.) to coordinate their initiatives, facilitate ongoing discussions on cybersecurity issues, and discuss potential joint projects and initiatives.

R2.2 Identify vulnerable groups and high-risk behaviour across the public to inform targeted, coordinated awareness campaigns.

R2.3 Intensify efforts in coordinated awareness campaigns to accelerate the growing proportion of Kosovar society that is aware of cybersecurity good practices. Consider providing coordinated social programmes for different age groups that will teach users about the safe and responsible behaviour online in their everyday use of the Internet, how to prevent any uncompromising behaviour, and how to report any incident.

R2.4 Make materials of such programmes freely accessible for the public in order to equip them with the right skills needed for their everyday use of Internet and online services.

R2.5 Promote the risk and threat understanding in the private sector and the prioritisation of cybersecurity, especially at executive level and among SMEs.

R2.6 Promote the sharing of information on incidents and best practices among organisations and across sectors to promote a proactive cybersecurity mind-set.

TRUST AND CONFIDENCE ON THE INTERNET

R2.7 Establish ISP programmes to promote trust in their services based on measures of effectiveness.

R2.8 Identify high-level risks affecting e-government services and prioritise cybersecurity in order to pre-empt and mitigate the number of occurrences. Ensure that security measures are in place for existing e-government services and new ones.

R2.9 Promote the use of e-government services through a coordinated programme, including the compliance to web standards that protect the anonymity of users. Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.10 Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

R2.11 Encourage users to access the terms and conditions for using e-commerce services and promote the posting of customer reviews (both good and bad) and testimonials.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.12 Guarantee enough resources for NAPPD to conduct inspections and control the fulfilment of the *Law No. 06/L-82 on the Protection of Personal Data.* Consider a technocracy management at the Council level, to promote the independency of this agency.

R2.13 Coordinate efforts and cooperation with organisations raising user awareness of online risks for personal information.

R2.14 Promote the understanding of protection of personal information online among users, the development of their skills to manage their privacy online, and privacy by default as a tool for transparency.

R2.15 Encourage a public debate regarding the protection of personal information to inform policymaking.

REPORTING MECHANISMS

R2.16 Encourage different stakeholders to coordinate the existing reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms. Victims of cybercrime should be able to report to the police by choosing different options: 1) dialling a number in case it is an emergency or the crime is in progress; and 2) completing an online form for non-emergency crimes or reporting via email. All reporting channels should offer the victim the option to report anonymously.

R2.17 Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.

R2.18 Raise awareness about the existing reporting mechanisms among the wider public and public and private sectors, and encourage their use as an investment in loss prevention and risk control.

MEDIA AND SOCIAL MEDIA

R2.19 In cooperation with organisations in the civil society, public agencies and media organisations, develop programmes and campaigns to raise awareness among media providers and leading social media actors.

R2.20 Encourage media and social media providers to further extend the coverage beyond threat reporting and focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts.

R2.21 Ensure that the debate in social and mainstream media informs policymaking.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

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

D 3.1 AWARENESS RAISING

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

Stage: Formative

Interviewed participants provided a long list of different awareness-raising programmes, courses, seminars, and online resources which are available for target demographics. Most of the given examples focused on children and young people under 18 years old. They see this demographic target not only as a key investment in the ICT skills of future workers, but also as a channel to pass cybersecurity information on to parents and families. The NCS 2016–2019 considers younger generations as an important target for the promotion of cybersecurity awareness and identifies the Ministry of Education, Science and Technology (MEST) as an institutional mechanism for the development of curricula on cybersecurity and organising awareness-raising activities.[53] This is reflected in the *Kosovo Education Strategic Plan (2017-2021),* which considers the use of ICT in class as part of its strategic objective on high-quality

[53] "National Cyber Security Strategy and Action Plan 2016-2019", MIA, accessed 15 June 2019, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/National_Cyber_Security_Strategy_and_Action_Plan_2016-2019_0.pdf.

teaching.[54] Through this plan, it has emphasised the need of ICT equipment and digital materials for students and teachers in schools. The plan also detects vulnerabilities such as a poor maintenance of ICT equipment, and a very limited number of teachers with the skills to integrate digital materials in class. To improve this situation, teacher development is prioritised through a licensing scheme that includes training (for instance, European Computer Driving License (ECDL) training), and school budgets contemplate organising training and professional support according to the needs of teachers. The plan also proposes development plans for maintenance and updating of ICT equipment. Although there is no direct budget for ICT maintenance, MEST has worked with the EU and US Agency for International Development (USAID) on maintaining ICT equipment in schools.[55]

The NCS 2016–2019 contemplates initiatives for raising awareness among younger generations, Internet end-users, and government employees. One of these initiatives is the European Cybersecurity Month. For this event, Prishtina hosted several activities such as lectures on security (University of Prishtina), a hacking challenge competition on vulnerability report (UBT-CERT),[56] and a training on cyber threats in a school (CACTTUS Education centre).[57] Kosovo also celebrates the Safer Internet Day, with various activities offered by different organisations that work towards building a safer online experience for children and young students. For example, the last programme contained international calls between students from Kosovar and British schools to share experiences when using the Internet, including their views on cyberbullying.[58] In 2018, UNDP organised an awareness campaign for online protection of young girls with an audience of some 100 parents, teachers and students. The Centre for Advanced Studies FIT is an example of an organisation that has conducted several educational projects to increase awareness on cybersecurity and its website aims to make the resulting materials accessible specially to children, parents, and teachers.[59] Another case is the private educational centre Bonevet, which foments awareness on cybersecurity to librarians through the Digital Citizen project.[60] Some organisations, such as Sense Cyber Research Centre and the ICT association STIKK, disseminate different materials online to raise awareness on different perspectives of cybersecurity; Sense offers a legal perspective[61] while STIKK offers the perspective of the ICT sector.[62] Finally, NAPPD has implemented several initiatives to raise cybersecurity awareness and is present in many platforms where this agency publishes activities that may raise awareness among the citizens (Facebook, Twitter

[54] “Kosovo Education Strategic Plan 2017-2021,“ MEST, accessed 15 October 2019, https://masht.rks-gov.net/uploads/2017/02/20161006-kesp-2017-2021-1.pdf.
[55] “Action plan of Kosovo education strategic plan 2017-2021”, MEST, accessed 4 November 2019, https://masht.rks-gov.net/uploads/2017/02/20161006-action-plan.pdf.
[56] “European Cybersecurity Month”, European Cybersercurity Month, accessed 15 October 2019, https://cybersecuritymonth.eu/ecsm-countries/republic-of-kosovo/hack-day-kosova-3.
[57] “Within cyber security month framework”, CACTTUS, accessed 15 October 2019, https://www.cacttus.com/cacttus/lajmet/within-the-framework-of-the-security-month-cacttus-visits-the-children-from-elementary-school-elena-gjika.
[58] “Safer Internet Day”, Safer Internet Day, accessed 15 October 2019, https://www.betterinternetforkids.eu/web/kosovo.
[59] “Internet and Security”, Internet and Security, accessed 4 November 2019, https://internetisigurte.org/en/.
[60]“Third workshop of the project Digital Citizen”, Bonevet, accessed 15 October 2019, https://www.bonevet.org/en/home-page-news/third-workshop-of-the-project-digital-citizen/.
[61] “Sense”, Sense, accessed 15 October 2019, https://sense.co.com/.
[62] “STIKK”, STIKK, accessed 15 October 2019, https://stikk.org/en/.

and website).[63] Some of these activities are providing guidelines on cybersecurity to employees in the health sector (health insurance institutions and regional hospitals) and employees in secondary education institutions (academic staff, school directors, and secretaries), giving some lectures at universities, collaborating with the media on privacy issues (for example, providing materials on legal changes related to privacy and participating in interviews), and planned activities for International Privacy Day.[64]

The stage of general awareness raising in 2019 has gained in maturity respect to the stage in 2015, because the NCS 2016–2019 has identified key population targets and includes initiatives for raising awareness. However, awareness campaigns usually have a limited budget because funding comes from different donors. Campaigns can only afford a small number of participants, which makes it difficult to make a significant impact on the population or extrapolate the awareness campaigns' conclusions to other contexts. The consulted stakeholders acknowledged the relevance of designing a national program for cybersecurity awareness that would coordinate efforts, reallocate budgets on these initiatives more efficiently, engage with new collaborators such as ISPs, and have a regular implementation in order to update its content according to new cybersecurity threats.

The cybersecurity awareness among executives has increased since 2015, although not significantly. The consulted stakeholders perceive that only executives of some sectors (such as ICT companies, banks, and branch offices of international companies) are aware of some cybersecurity risks for their organisations and take responsibility on it. In such cases, executives follow international standards on good practices. However, this is not the case when looking at all sectors.

D3.1 Awareness Raising (*assessed in D2.2 and D3.4 in CMM Report Kosovo 2015*)

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ The NCS contains awareness-raising programmes for strategic population targets ↑ Some awareness-raising activities are linked to international initiatives	→ Executives of leading sectors (ICT highly developed) are aware of their responsibility on the cybersecurity risks of their organisations	! No measurement of the effectiveness of awareness campaigns ! Need of additional coordination of activities towards a national awareness programme ! Need to raise awareness at the executive level within the public and private sectors where ICT is not highly developed

Maturity Levels in Comparison 2015 : 2019

2015 – Start-Up and Formative | **2019 – Formative**

[63] "National Agency for Personal Data Protection", APPD, accessed 15 October 2019, http://www.amdp-rks.org/?page=2,10,167#.XbA_XOhKjD4.

[64] "Annual Work Report 2018", APPD, accessed 15 September 2019, http://www.amdp-rks.org/repository/docs/ENG___Raporti_Vjetor_i_Pun__s_p__r_2018_2232019.pdf.

D 3.2 FRAMEWORK FOR EDUCATION

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

Stage: Formative

Since 2011, the Kosovar pre-university education system has implemented competency-based curricula, including the integration of ICT in students' learning processes, and the responsible and effective use of ICT and media.[65] Accordingly, the NCS 2016–2019 considers the inclusion of a dedicated cybersecurity component and modules on online risks in these curricula. However, some schools have problems integrating ICT-related competences because, according to the *Kosovo Education Strategic Plan 2017-2021*, only 44.4 percent of schools have ICT equipment and, as mentioned in D3.1, there is a shortage of ICT skills among teachers.

Most universities in Kosovo offer different study programmes in fields related to cybersecurity in both English and Albanian. According to the Kosovo Accreditation Agency,[66] there are seven universities (University of Applied Sciences, University of Gjilan, University of Prishtina, AAB College, Riinvest College, UBT College, and Universum College) offering Master and Bachelor degrees in fields related to cybersecurity (Computer Science, Telecommunications, Engineering and Informatics, etc.). Only AAB College has an accredited professional Bachelor's degree specialising in cybersecurity. Regarding the research activity, the NCS 2016–2019 acknowledges the importance of research and development on IT security as a response to cybersecurity threats. However, research activity in Kosovo is in an earlier stage,[67] and only the University of Prishtina offers a PhD programme in a field related to cybersecurity, the PhD in Management and Informatics.

In addition to universities, Kosovo has 68 Vocational Education and Training (VET) schools that offer different programmes, one of them the ICT program. For the 2018–19 course, this programme had 11 percent of VET students and was the fourth most popular program after Engineering, Manufacturing and Construction (33%) Business, Administration and Law (28%)

[65] "Curriculum framework for pre-university education in the Republic of Kosovo", International Bureau of Education, accessed 5 November 2019, http://www.ibe.unesco.org/fileadmin/user_upload/archive/curricula/kosovo/kv_alfw_2011_eng.pdf.

[66] "List of accredited study programmes,"Kosovo Accreditation Agency, accessed 15 October 2019, http://akreditimi-ks.org/docs/Downloads/Accreditation/kshc20092019/kshc20092019.pdf.

[67] "The situation of research in Kosovo", Kosovo Education and Employment Network, accessed 15 October 2019, http://www.keen-ks.net/site/assets/files/1458/the_situation_of_research_in_kosovo_eng-1.pdf.

and Health and Welfare (18%).[68] CACTTUS Education is a professional school that offers two-year study programs in ICT, in addition to professional training and a course in technology for children. [69]

During consultations with stakeholders, participants mentioned that ICT professionals are scarce in Kosovo, and the current framework is not providing the right incentives to promote education in cybersecurity. ICT professionals who studied in Kosovo find better career prospects abroad and many of them emigrate. Those ICT professionals who decide to remain in Kosovo are attracted by the higher salaries of the private sector, and the public sector is the most affected part of this shortage of ICT skilled workers. It also affects the limited availability of experts who can train. This situation was already revealed in 2015 by a STIKK survey of firms;[70] the highest percentage of participants (36%) agreed that there was a shortage of labour supply for skilled ICT professionals. Overall, the current educational framework for cybersecurity has not changed much since 2015 and indicates a *formative* maturity stage.

D3.2 Framework for Education (*assessed in D3.1 and D3.2 in CMM Report Kosovo 2015*)

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
	→ The NCS and the MEST prioritise cybersecurity in the pre-university education system → Kosovar universities offer a range of study programmes in fields related to cybersecurity	! More resources are needed to implement ICT-related competences in all Kosovar schools ! Shortage of labour supply for skilled ICT professionals

Maturity Levels in Comparison 2015 : 2019

2015 – Formative | 2019 – Formative

[68] “Vocational education and training in Kosovo”, Kosovo Education and Employment Network, accessed 15 October 2019, http://www.keen-ks.net/site/assets/files/1470/vet_education_in_kosovo_challenges_and_opportunities_eng.pdf.
[69] “Cacttus Education”, CACTTUS, accessed 15 September 2019, https://cacttus.education/en.
[70] “Mapping of ICT sector”, STIKK, accessed 15 October 2019, ”https://stikk.org/wp-content/uploads/2018/11/Publications_2015_-_Skills_Gap_EN.pdf.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

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

Stage: Formative

One of the objectives of the 2016–2019 NCS is institutional development and capacity building, including the human capacity building of all institutions involved in the strategy. For all these institutions, the NCS considers the development of training curricula and the harmonisation of training across institutions to improve coordination and cooperation. A mention is made of the requirement of appropriately trained personal in CERTs/CSIRTs, and on the need to provide professional education and training for police specialists and law enforcement bodies combating cybercrime. MED is the institutional mechanism of the NCS that encourages the development of training in ICT.

According to the consultations with stakeholders, Cyber Academy is the best professional school of cybersecurity for training cybersecurity engineers and professionals.[71] This school offers a one-year programme in cybersecurity and cyber warfare, including modules in different topics of cybersecurity (cryptography information security, advanced penetration testing, cybercrime investigation, etc.). Specialist training on topics not offered by Cyber Academy would need to be done in another country. For example, the KP, the MIA, Kosovo Prosecution Office, Police Inspectorate and Kosovo Correctional Service recently completed a one-week course offered by the International Criminal Investigative Training Assistance Program (ICITAP).[72] Other notable institutions that offer courses on cybersecurity for cybersecurity professionals and non-cybersecurity professionals are the Innovation Centre Kosovo (ICK)[73], AUK Training & Development Institute,[74] and CACTTUS Education.[75] Civil servants and workers in the public administration are offered training by the Kosovo Institute for Public Administration (KIPA). However, according to the consulted stakeholders, its training focuses on gaining ICT skills rather than cybersecurity.

There is a long list of professional training centres and academies that offer a wide range of ICT certification schemes (Cisco, Microsoft, Oracle, etc.). However, these certifications do not always share the same standards. Abazi and Hajrizi (2018) illustrate this problem in their study

[71] “CA-Professional”, Cyber Academy, accessed 15 September 2019, https://cyberacademy.co/cybersecurity-program/.

[72] “International Criminal Investigative Training Assistance Program (ICITAP)”, The United States Department of Justice, accessed 15 October 2019, https://www.justice.gov/criminal-icitap.

[73] “Courses”, ICK, accessed 15 October 2019, https://ickosovo.com/training/courses.

[74] “Courses”, AUK Training & Development Institute, accessed 5 November 2019, http://tdi.auk.org/courses/.

[75] “Professional training”, CACTTUS, accessed 5 November 2019, https://cacttus.education/en/professional-training/.

on the qualification system for ICT workers in Kosovo.[76] There were 134 workers participating in the study and they certified their qualifications with 60 different certification systems. The authors conclude that there is a lack of transparency concerning qualifications while not all training and professional qualifications are capable enough to meet the demands for a rapid change of the labour profiles. This point was also raised during the consultations with stakeholders.

In general, the consulted participants noticed no evidence of how trained workers internalise the gained skills and transfer them to other employees in the public sector. However, in the private sector, companies that invest in employee training usually measure the return of their investment. Overall, the training framework in cybersecurity training has not changed much since 2015.

D3.3 Fram. for Professional Training (*assessed in D3.1 and D3.3 in CMM Report Kosovo 2015*)

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
	→ There is a wide range of courses that offer ICT professional certification and cybersecurity training	! Problem of retention of cybersecurity- and ICT-skilled workers ! Need for additional efforts to build a cadre of cybersecurity-specific professionals ! No evidence of metrics evaluating take-up of courses

Maturity Levels in Comparison 2015 : 2019

2015 – Formative	2019 – Formative

[76] Blerton Abazi and Edmond Hajrizi, "Research on the Importance of Training and Professional Certification in the Field of ICT Case Study in Kosovo", *IFAC-PapersOnLine* 51, no. 30 (2018), 336–339, https://doi.org/10.1016/j.ifacol.2018.11.327.

RECOMMENDATIONS

Following the information presented in the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to Kosovo. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC CMM.

AWARENESS RAISING

R3.1 Appoint a designated body or organisation to lead and coordinate the cybersecurity awareness-raising programme at a national level and ensure the necessary budget for doing so.

R3.2 Task the appointed designated body to develop and deliver a national cybersecurity programme in cooperation with relevant stakeholders from public and private sectors, including ISPs, using international best practices in this area as guidance.

R3.3 Task the appointed designated body to develop a national portal to inform on the different cybersecurity awareness programmes conducted in Kosovo and disseminate the cybersecurity awareness programme via this platform.

R3.4 Task the appointed designated body to develop and implement evaluation measurements to study the effectiveness of the awareness programmes at a level where they inform future campaigns, taking into account gaps or failures.

R3.5 Ensure that schools with ICT equipment maintain and update this equipment with a regular budget dedicated to it.

R3.6 Develop a national awareness programme for teachers, to increase their capabilities to prepare and use electronic content.

R3.7 The design of the national awareness programme for teachers (R3.6) should consider the needs of schools in achieving the objectives of the education strategic plan 2017–21.

R3.8 Develop a national awareness programme for executive managers within the public and private sector (specially SMEs), dealing with the identification of cybersecurity risks and threats in companies, and good practices to minimise such risks.

FRAMEWORK FOR EDUCATION

R3.9 Intensify efforts in integrating ICT equipment in all Kosovar primary and secondary schools and ensure that the growing access to ICT in schools goes with a growing teachers' capability to work with ICT equipment.

R3.10 Task the MEST, or any other relevant body, to consolidate cybersecurity education priorities on all levels through broad consultation across government, private sector, academia, and civil society, informed by the NCS and the Education Strategic Plan.

R3.11 Task the appointed body to study the increment of specialised cybersecurity degrees offered in universities and other higher education bodies.

R3.12 Task the appointed body to develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators to ensure that skilled staff are available to teach newly formed and existing cybersecurity courses. As many students in Kosovo are fluent in English, there is an opportunity to bring in English-speaking professors from abroad and fill any gap in the education framework.

R3.13 Intensify resources for national cybersecurity research and laboratories to encourage the development of PhD programmes in different universities.

R3.14 Task the appointed body to develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment.

R3.15 Inform targets of population (young workers, unemployed workers, students of secondary schools, university students, etc.) about the demand for ICT-skilled workers in the Kosovar labour market.

R3.16 Create incentives to study ICT-related programmes at different levels (vocational programmes, Bachelor and Master's degrees, professional training, etc.) such as subsidies or zero-interest loans to finance education costs.

R3.17 Encourage initiatives that incentivise the retention of cybersecurity and ICT professionals in Kosovo. For instance, inform executive managers in the public and private sector about the value of ICT professionals who fight against cyber threats and risks in corporations.

R3.18 Create career incentives to attract and retain cybersecurity and ICT professionals in the public sector. For example, offer a salary scheme and a career development path that competes positively with the opportunities offered in the private sector.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.19 Task the MED, or any other relevant body, to encourage the standardisation of the existing training for security professionals towards a unique certification system, one where all certifications are comparable.

R3.20 Task the appointed body to advance the role and importance of cybersecurity certification in IT job categories, including possible regulation to this effect such as requirements for specific job roles. Encourage employers to train staff to become cybersecurity professionals and to encourage retention after training, create career incentives for cybersecurity employees within the public and private sector.

R3.21 Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

R3.22 Begin to implement metrics that evaluate the take-up of *ad-hoc* training courses, seminars, online resources, and certification offerings.

R3.23 Intensify efforts in leading government agencies and leading firms in the industry to prioritise cybersecurity; extend to all ministries/industrial sectors, efforts that promote the understanding and identification of cyber risks and threats.

R3.24 Extend training programmes to most employees at all levels in the private and public sector, establishing continuous training on cybersecurity issues. International best practices and documents for professional training should form the basis of these courses.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

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

D 4.1 LEGAL FRAMEWORKS

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

Stage: Formative

At the time of this assessment, Kosovo had not yet enacted any overarching law specifically concerning ICT security. A comprehensive cybersecurity bill, however, is under preparation, with drafting efforts being led by the MIA. At the sectoral level, the *Law on Electronic Communications*,[77] developed under the direction of the MED and adopted in 2012, addresses select ICT security aspects with a narrower focus on operators of electronic communications networks and service providers. The law organises the registration of service providers but also establishes regulatory authorities to manage the provision of electronic communication services and competition within the sector and provided the legal basis for the later creation of the national CERT in 2016 (Art.10.21). As such, the law sets forth obligations for operators to ensure the confidentiality, integrity and availability of their services. Art.85 of the law vests telecoms regulator ARKEP with the authority to issue regulations on technical and organisational security measures and sets auditing and breach notification requirements. To

[77] Law on Electronic Communications of 2012, no. 04/L-109, Official Gazette of the Republic of Kosovo 30/2012, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2851.

this end, the law foresees the adoption of additional sub-legal acts and regulations to implement these provisions. Actual regulations[78] mandating the reporting of major security incidents and the completion of security audits only came into effect in 2016 (see section D5.1 of this report on Adherence to Standards for additional details). These regulations were supported by specifications of Minimal Technical Measures for Security and Integrity of Electronic Communication Networks and/or Services.

At the time of writing, the MIA was reported to be working on a new comprehensive cybersecurity law with ambitions to also overhaul the 2010 *Law on the Prevention and Fight of Cybercrime*. As representatives of the MIA were not able to attend the stakeholder consultations conducted in Kosovo for this assessment, details on the scope and content of this first dedicated cybersecurity law could not be fully ascertained. While representatives of the defence and banking sectors were involved in consultations for the law, plans for the law—as presented by interviewed stakeholders—suggest that the scope of the law will not address cybersecurity considerations for the defence and banking sectors. The law is reportedly slated to include provisions for creating a national cybersecurity agency, although this proposal has met with concerns from other cabinet-level agencies (as expressed during consultations for this assessment) about possible confusion in the division of competencies and efficiency in the use of public resources. Kosovo's larger ISPs have been invited to participate in consultations to inform the drafting of this new law. Feedback from these consultations has been collected by the MIA. Representatives of major actors in Kosovo's energy and transportation sector, on the other hand, were not aware of any opportunity to weigh in but expressed willingness to contribute if they were approached. The latter group voiced concerns about their limited awareness regarding the legislative plans and wished for more information to be in a position to adapt to the new law in time. MIA representatives indicated plans to submit a draft of the law for public consultation, open to representatives from all sectors. Opportunities for all relevant stakeholders to provide input for consideration during the drafting phase not only help ensure inclusive policy-making but also reduce the potential for any friction or delay in the implementation phase.

Given its parliamentary democracy system, the vast majority of legislative proposals in Kosovo originate from government initiatives. With ambitions to align itself with the legal framework of the EU, transposition of EU legislation is a key driver of legislative activity in Kosovo. In the past, transposition projects have stalled and led to the frequent revision of legislation as key provisions explicitly included in draft laws to comply with EU frameworks were removed from bills during parliamentary debate, even as ministries responsible for the draft explained linkages to the EU *acquis communautaire*. These dynamics can set up laws for revision the moment they are passed and require careful management in the planned transposition of the Directive on security of network and information systems (NIS Directive, see section D1.3 of this report on Critical Infrastructure Protection for additional details).

Freedom of expression online is not explicitly regulated in Kosovo.[79] Fundamental rights, including freedom of speech, however, are regularly referenced in legislation on electronic

[78] ARKEP, Regulation on Technical and Organisational Standards for Security and Integrity of Electronic Communication Networks and/or Services, Prot. No. 046/B/16.

[79] European Commission, "EU Enlargement Package: Freedom of Expression – Information Society and Media 2019," 2019, 10, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/freedom_of_expression_2019.pdf.

communications or digital data protection as foundational building blocks. The 2015 *Law on the Interception of Electronic Communications*,[80] for instance, cites "respect for human rights and fundamental freedoms recognised and guaranteed by the Constitution and the European Convention on Human Rights and Freedoms, including the interpretation by the European Court of Human Rights through its judicial practice" as guiding principles (Art.4.1.1). The 2019 *Law on the Protection of Personal Data* lays claims to being drafted in compliance of the EU General Data Protection Regulation (GDPR),[81] thus commanding the law by extension to "respect all fundamental rights and observe[s] the freedoms and principles recognised in the Charter[82] as enshrined in the Treaties,[83] in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."[84] In addition, the *Law on the Protection of Personal Data* reinforces the role of the NAPPD in promoting and supporting fundamental rights on personal data protection (Art.64.1.4). While formally limited to regulating the responsibilities of audio and audio-visual media services, the Independent Media Commission (IMC) has been tasked with the development of a *Strategy of Digitalization for Terrestrial Broadcasting*. The *Code of Ethics for Media Service Providers* issued by the IMC in 2016 applies to all licensed media service providers to guarantee freedom of expression based on the principles recognised in the constitution of the Republic of Kosovo, the Universal Declaration of Human Rights, and the European Convention on Human Rights.[85]

In February 2019, Kosovo enacted a new *Law on Protection of Personal Data*,[86] abrogating previous umbrella legislation on data protection (Law No. 03/L-172) that had been adopted in 2010. While the law of 2010 already required organisations to report data breaches within clearly defined reporting periods, the new legislation that came into force in 2019 aspires, as mentioned above, to be a full transposition of the GDPR, drawing on the expertise of EU legal officers who were part of the working group that prepared first drafts of the law.

In key provisions, the 2019 law adopts, verbatim, the six lawful bases for the processing of personal data as set forth by the GDPR (Art.5), recognises the right to erasure ("the right to be forgotten," Art. 16), the right to data portability (Art.19), and defines the circumstances that need to lead to the designation of a data protection officer, as well as their tasks and responsibilities (Chapter X). Under the law, all data subjects have the right to file a complaint with the NAPPD where they suspect that the processing of their data is in violation of the law (Art.52). A personal data breach generally needs to be reported to the NAPPD within 72 hours

[80] Law on the Interception of Electronic Communications of 2015, no. 05/L-030, Official Gazette of the Republic of Kosovo 18/2015, https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968.

[81] Law on the Protection of Personal Data of 2019, no. 06/L-082, Official Gazette of the Republic of Kosovo 6/2019, Art.1.2, https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616.

[82] The Charter of Fundamental Rights of the European Union

[83] EU treaties, see https://europa.eu/european-union/law/treaties_en.

[84] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1, http://data.europa.eu/eli/reg/2016/679/oj.

[85] Code of Ethics for Media Service Providers in the Republic of Kosovo of 2016, IMC-2016/03, Art.2, https://kpm-ks.org/assets/cms/uploads/files/Legjislacioni/1493714855.8029.docx.

[86] Law on the Protection of Personal Data of 2019, no. 06/L-082, Official Gazette of the Republic of Kosovo 6/2019, https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616.

after its detection by the affected entity. Notification has to include descriptions of the likely consequences that might result from the breach, and the mitigation measures that have been implemented or are under consideration to reduce these effects (Art.33). Where a data breach is holding the rights and freedoms of a person at high risk, the data subject is to be made aware of the data breach within the shortest delay (Art.34). The law establishes rules for the transfer of personal data to other countries and tasks the agency with developing and maintaining a list of countries that provide adequate levels of data protection (Chapter XI). The law positions the NAPPD to conduct inspections and audits on its own initiative to investigate compliance with data protection requirements and to impose fines for detected violations (Art.68). To this end, the law classifies a spectrum of punitive measures (Chapter XXI) for instances of non-compliance, ranging from minor offences to serious violations. In line with GDPR provisions, in cases of serious and great violation of personal data, the NAPPD may assign fines of up to four percent of general turnover (Art.105).

The NAPPD, the agency responsible for monitoring the implementation of the *Law on Protection of Personal Data*, operates as an independent entity that is also tasked with inspecting all government departments. The agency is led by a council convening the Chief National Supervisor and four national supervisors who are elected by the Kosovo Assembly. The governing council is currently supported by a staff of 18 civil servants. None of these staff members has a professional background related to IT security. To fulfil the additional responsibilities entrusted to it by the new law and to develop expertise to assess the security measures taken by data controllers under its supervision, the agency has expressed the need for an increased number of appropriately qualified staff.

To set the scene for the conditions under which the NAPPD is assuming these new responsibilities, it is worth quoting directly from the agency's Annual Report for 2018: "Since June 2011, the Agency has operated with a limited budget, a small number of staff, and for these reasons not fully functionalised or established departments foreseen by the organisational structure."[87] Noting severe resource constraints, the NAPPD warned that "it is almost unrealistic to expect the fulfilment of the desired objective of achieving the appropriate level of knowledge of citizens about their rights to protect personal data – privacy and access to public documents – transparency[sic], if the necessary funds for the realisation of raising awareness campaigns are missing."[88] The Annual Report also notes a 30 percent reduction in the initial budget allocated to the NAPPD for 2018,[89] a significant cutback at a time when the agency objectively requires additional resources and characterises the completion of its mission as regards the direct imposition of fines for violations of the law as a "continuous challenge".[90] At the time of this assessment, the agency had not been able to conduct inspections for three years. Inspections ceased in June 2016 when the mandate of national supervisors expired. When the last inspections were conducted, companies headquartered in EU countries were, by and large, found to be complying with provisions under the previous data protection law. No statistics about assigned fines are publicly available. The European Commission in July 2019 published a call for proposals aimed at

[87] National Agency for Protection of Personal Data, "Annual Work Report 2018," March 2018, 12, https://www.amdp-rks.org/repository/docs/ENG___Raporti_Vjetor_i_Pun__s_p__r_2018_2232019.pdf.

[88] Ibid.

[89] Ibid., 31.

[90] Ibid., 32.

"Strengthening the Information and Privacy Agency in Kosovo," supported by the commitment of a project grant to the amount of €2 million.[91] The call invited EU member states to present proposals for a twinning initiative that would pair the NAPPD with one of their EU counterparts, to assist the agency in its institutional capacity-building and efforts to raise public awareness on data protection.

Serious concerns were expressed during consultations for this assessment, that companies might take advantage of the NAPPD's current lack of capacity to send out inspectors to confirm their compliance with breach notification obligations. Individual complaints can be verbally filed with the agency by telephone, as well as in writing and via an online submission form.[92] Over the course of 2018, the agency has received 42 complaints, continuing the downward trend of the last four years. These statistics, however, reflect circumstances before the new *Law on Protection of Personal Data* came into force.

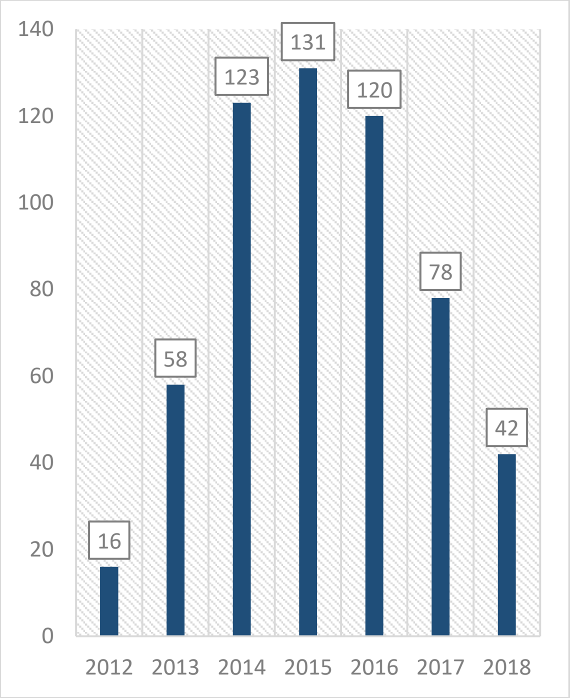

Figure 3: Individual complaints submitted to NAPPD on an annual basis[93]

In the past, the five members of the agency's governing council were entrusted with conducting inspections. Under the new data protection law, inspections will no longer be carried out by political appointees but by specialised civil servants directly recruited by the NAPPD and led by a commissioner who is selected and confirmed by members of the National Assembly. The new position of commissioner, created by the 2019 data protection law, was

[91] "Strengthening the Information and Privacy Agency in Kosovo," EuropeAid/165740/DD/ACT/XK, International Cooperation and Development – Calls for Proposals and Tenders, European Commission, 12 July 2019, https://webgate.ec.europa.eu/europeaid/online-services/index.cfm?ADSSChck=1571938971685&do=publi.detPUB&searchtype=QS&aoref=165740&page=1&orderbyad=Desc&nbPubliList=50&orderby=upd&userlanguage=en.

[92] Online Form to File Complaints with the NAPPD, NAPPD, accessed 1 November 2019, https://www.amdp-rks.org//?page=2,6.

[93] NAPPD, "Annual Report 2018," 21.

expected to be filled in the second half of 2019. A shortlist of candidates for the position was to be prepared by a selection panel appointed by the Parliamentary Committee for Security of the National Assembly that is to be put to vote by the Assembly (Art.60.4).[94] Vested with a five-year renewable mandate, the commissioner wields critical influence to shape the regulatory landscape. With this in view, stakeholders interviewed for this assessment recommended that the Committee appoint professionals in the field to the selection panel, to ensure the identification of qualified candidates. The incoming commissioner has to issue a sub-legal act on the functioning of the agency following the enactment of the new law for inspections to start again (Art.58.7). This starting condition makes the confirmation of a commissioner a priority task.

In addition to the abovementioned responsibilities, the NAPPD consults government departments on data protection aspects of their legislative projects. In 2018, the NAPPD offered legal opinion on 27 draft laws, 13 draft regulations and 47 drafts of administrative instructions.[95]

In parallel to GDPR provisions, the *Law on the Protection of Personal Data* assigns particular importance to the protection of data of children (Art.5.1.6). These additional rules apply specifically to the provision of online services, including social media, and introduce age thresholds and parental responsibility in giving consent to data processing (Art.7).

In June 2019, the National Assembly adopted a new *Law on Child Protection*,[96] which is set to enter into force in June 2020. Sections of the law pertaining specifically to child protection online primarily concern access limitations and advisories on potentially harmful content, including steps to close off online gambling platforms to minors (Art.44.1). The law requires electronic and online media and Internet portals to actively implement child-protection measures, including awareness-raising efforts to inform on potentially negative effects of exposure of children to certain media products (Art.45.3). Kosovo's main ISPs generally offer parental control options, allowing parents to choose among different filter settings designed to block webpages that are known to contain or host illegal content, pornography, malware or gambling activities. Public institutions are under further obligation to ensure safe use of the Internet, including filtering and access restrictions for websites hosting content unsuitable for children. Yet, these provisions only apply to Internet use in public spaces (Art.53.1). The law tasks the MEST and local educational organisations with taking measures to advance child protection online, in particular through training on the responsible the use of connected devices (Art.37.5.11). To fully implement online protection measures set out in the law, the MIA has been charged with drafting a sub-legal act to specify additional measures to shield children from pornographic content; prosecute online child abusers; reduce the exposure of

[94] The British Embassy in Pristina has agreed with the Government and Assembly of Kosovo to offer technical assistance in support of the recruitment processes of 42 senior officials in the civil service and independent institutions, with the purpose of strengthening transparency, meritocracy and good governance. The commissioner of the NAPPD is one of the 42 recruitment processes identified in the memorandum of understanding between the UK and Kosovo. The recruitment process of the commissioner can be tracked online via the project's website, Kosovo Selection: https://www.kosovoselection.org/central.

[95] NAPPD, "Annual Report 2018," 16.

[96] Law on Child Protection of 2019, no. 06/L-084, Official Gazette of the Republic of Kosovo 14/2019, https://gzk.rks-gov.net/ActDetail.aspx?ActID=20844.

children to health- and life-threatening material; and to provide assistance to children at risk of other forms of online harm (Art.53.3).

In addition to sections of the Criminal Code (Art.232), the *Law on the Prevention and Fight of Cybercrime* contains specific provisions that foresee prison sentences for the production, provision, distribution, procurement and possession of child pornography where these acts involve computer systems (Art.16).

In 2015, the Kosova Education Center, a not-for-profit organisation, was commissioned by the Government of Kosovo to develop a Strategic Plan for Protection of Children from Risks of the Internet (2015–19) to explore child protection measures with a particular focus on online harms. Adoption of the Strategic Plan was scheduled for 2016 but has since been deferred indefinitely.

Consumer protection legislation in Kosovo is largely seeking to conform with EU law. Kosovo adopted a new *Law on Consumer Protection* in June 2018, which effectively transposes EU legislation on consumer protection (Art.1.2). In line with this practice, it is expected that Kosovo will revise its legislation to reflect the measures proposed by the European Commission in April 2018 under its New Deal for Consumers,[97] including steps to strengthen the enforcement of consumer rights in the digital economy. Any upcoming review of laws will likely also consider the EU's 2019 Directive on contracts for the supply of digital content and digital services,[98] intended to enhance the legal protection of consumers and traders in cross-border commerce. The present law does not contain any provisions that particularly address consumer protection online but it could be applied by drawing on established practices in EU member states for implementing and enforcing the transposed EU Directives on which Kosovo's *Law on Consumer Protection* is based. In cases where a delivered product or service does not align with the purchase agreement, consumers—in addition to filing a complaint with the trader—can submit their case[99] to the Consumer Protection Department under the Ministry of Trade and Industry. Kosovo is also currently in the final steps of transposing the EU Regulation on Electronic Identification and Trust Services for Electronic Transactions (eIDAS).[100] The draft law, prepared by the MED, has passed public consultation and is scheduled for submission to Parliament for approval.

[97] "Review of EU Consumer Law – New Deal for Consumers," European Commission, accessed 1 November 2019, https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en.

[98] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, Official Journal of the European Union L 136/1, http://data.europa.eu/eli/dir/2019/770/oj.

[99] Online Form for Submitting Consumer Protection Complaints, Ministry of Trade and Industry of the Republic of Kosovo, accessed 1 November 2019, https://konsumatori.rks-gov.net/complaintPost.php.

[100] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257/73, http://data.europa.eu/eli/reg/2014/910/oj.

An array of laws regulate various aspects of intellectual property protection severally, including the *Law on Copyright and Related Rights*[101], the *Law on Patents*,[102] the *Law on Industrial Design*[103] and the Criminal Code. These laws are not specific to the protection of intellectual property online but are broad in scope to admit for general application independent of the medium. Much like for other domains, Kosovo's legislation on intellectual property rights and their protection is aligned with EU legal frameworks. The Office of Industrial Policy under the Ministry of Trade and Industry and the Office of Copyright and Related Rights under the Ministry of Culture, Youth and Sports are responsible for registering rights and designs. Neither office holds executive powers and claims regarding the violation of rights are relegated to the court system or relevant sectoral regulator. The IMC in 2013 issued a specific Regulation on Copyright[104] that complements the *Law on Copyright* in its application to broadcasts of audio and audio-visual media services licensed by the IMC.

In 2010, Kosovo enacted the *Law on the Prevention and Fight of Cybercrime*,[105] which serves as the main legal text on substantive matters of cybercrime. The law addresses a range of crimes violating or endangering the confidentiality, integrity and availability of computer data and systems, including illegal access of computer systems, unauthorised interception or transfer of data, interference with the functioning of computer systems and the general misuse of devices. Covered under the law are also certain related offences such as cyber-enabled forgery and fraud.

While Kosovo is not a signatory to the Budapest Convention on Cybercrime, a section-by-section comparison prepared by the CoE within the framework of the organisation's capacity-building programmes shows[106] that all core components of the Budapest Convention have been codified into law in Kosovo, either as part of the cybercrime law or as part of the Criminal Code, the *Law on Electronic Communications* or multiple laws covering procedural elements—albeit not always to the same level of detail as laid out in the Convention.

In the view of several of the stakeholders consulted, including government officials and international partners, the present cybercrime law addresses only a minimal set of cybercrimes and cyber-enabled criminal offences and is considered to be in need of revision to reflect technological advances and related evolutions in criminal behaviour. Interviewed participants submitted that without specialised training, judges might not apply the cybercrime law even in straightforward cybercrime cases and instead, resort to provisions in the Criminal Code. In this respect, participants cautioned that changes to the Criminal Code might receive more attention from judges, prosecutors and law enforcement and saw the

[101] Law on Copyright and Related Rights of 2011, no. 04/L-065, Official Gazette of the Republic of Kosovo 27/2011, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2787.

[102] Law on Patents of 2011, no. 04/L-029, Official Gazette of the Republic of Kosovo 12/2011, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2756.

[103] Law on Industrial Design of 2015, no. 05/L-058, Official Gazette of the Republic of Kosovo 50/2015, https://gzk.rks-gov.net/ActDetail.aspx?ActID=11329.

[104] Regulation on Copyright of 2013, IMC 2013/02, https://kpm-ks.org/assets/cms/uploads/files/Legjislacioni/1426064654.4935.doc.

[105] Law on the Prevention and Fight of Cybercrime of 2010, no. 03/L-166, Official Gazette of the Republic of Kosovo 74/2010, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2682.

[106] "Legislative Profile – Kosovo," Octopus Cybercrime Community, Council of Europe, accessed 1 November 2019, https://www.coe.int/en/web/octopus/country-legislative-profile/-/asset_publisher/LA6eR74aAohY/content/kosov-3.

adoption of a new version of the Criminal Code in early 2019 as a missed opportunity to introduce corresponding amendments.

This task of revising existing cybercrime legislation has fallen to the MIA, which has been formally charged with updating the law. At the time of writing, it remained unclear whether these revision plans would result in a stand-alone law that seeks to clarify and extend the current law based on the Budapest Convention or if the new cybercrime provisions will form part of the new comprehensive cybersecurity legislation likewise under preparation by the MIA.

Procedural aspects of Kosovo's cybercrime legislation are largely codified in the Criminal Procedure Code (Chapter IX).[107] Art.17 of the *Law on the Prevention and Fight of Cybercrime* includes special provisions to expedite securing data relevant to an investigation where reasonable cause exists to believe electronic evidence might be destroyed or manipulated. These provisions enable investigators, prosecutors and courts to approach service providers with requests to preserve user and traffic data directly related to an ongoing investigation for defined periods of time and ensure the partial disclosure of traffic data where data is distributed among several providers. Additional procedural elements establishing authorities to request subscriber information and Internet connection logs from communication service providers are detailed in the *Law on Electronic Communications* (Art.68 and Art.104).

D4.1 Legal Frameworks

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ Adoption of new data protection legislation that broadly transposes GDPR provisions	→ Review of cybercrime legislation, with narrow stakeholder participation → Umbrella law on cybersecurity under discussion → Legislation on fundamental rights, child protection, intellectual property and consumer protection applies offline and online; jurisprudence that applies these laws to online cases remains limited → Preparations for transposition of NIS Directive are underway	! NAPPD faces critical resource shortage and mandated inspectors to carry out reviews of compliance data protection requirements

Maturity Levels in Comparison 2015 : 2019

2015 – Formative | 2019 – Formative

[107] Criminal Procedure Code of 2012, no. 04/L-123, Official Gazette of the Republic of Kosovo 37/2012, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2861.

D 4.2 CRIMINAL JUSTICE SYSTEM

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

Stage: **Formative to Established**

The Kosovo Police (KP) operates a specialised unit under the Directorate for Investigation of Organised Crime that is tasked with the investigation of cybercrime. The Kosovo Forensic Agency lends additional investigatory support with the evaluation of electronic evidence.

Art.7 of the *Law on the Prevention and Fight of Cybercrime* recognises the need for continuous training of investigators, prosecutors and members of the judiciary who are charged with fighting cybercrime. The Police Inspectorate of Kosovo, however, cautions that rapid technological evolutions pose challenges for trainers to keep up. Several stakeholders among participants consulted for this assessment deemed training with focus on specific technological challenges at risk of becoming outdated and losing value fast, unless complemented by appropriate contextualisation that includes continuities in tactics that persist throughout technological changes. In the view of this group, investigative capabilities of Kosovo's authorities lagged several years behind in the implementation of internationally recognised best practices. In combination with the technology-specific approach to training, new capabilities are at risk of being already circumvented or outperformed by threat actors when they become available. An EU-funded project currently supports the KP and Kosovo Forensic Agency in the assessment of their needs of specialised equipment.[108] Following this assessment, the project will facilitate the procurement of identified toolkits along with the necessary training to develop the capacities to leverage the equipment for the effective prevention and investigation of cybercrime.

Starting in 2016, the CoE has been implementing iPROCEEDS, a project jointly funded with the EU to reduce the effects of cybercrime across the region of south-eastern Europe and Turkey.[109] Supported by €5.56 million, the project facilitated a range of national and regional capacity-building activities up until its conclusion in June 2019.

iPROCEEDS organised training and consultations aimed at strengthening legislation and the ability of authorities in the project region to search and seize gains from cybercrime. The project assisted cybercrime units in developing means for national cooperation (with supporting investigators, including from financial intelligence units) and for international cooperation and

[108] "Assistance to Kosovo Forensic Agency and Kosovo Police to Improve Special Investigation Techniques," European Union Special Representative in Kosovo, accessed 1 November 2019, https://kosovoprojects.eu/project/assistance-to-kosovo-forensic-agency-and-kosovo-police-to-improve-special-investigation-techniques/.

[109] iPROCEEDS (3156)–Cooperation on Cybercrime under the Instrument of Pre-accession (IPA): Project on targeting crime proceeds on the Internet in south-eastern Europe and Turkey, Project Summary, Council of Europe, 20 February 2019, https://rm.coe.int/3156-iproceeds-summary-v5/1680932de1.

information sharing with other cybercrime units. To this end, the project has focused on establishing and improving publicly available mechanisms for the reporting of online fraud and other cybercrime as well as platforms for information sharing between the public and private sectors. To sustain training impact, the project has invested in building up capacity in national judicial training academies to ensure the continued provision of training on cybercrime and electronic evidence handling.

Activities sponsored by iPROCEEDS in Kosovo in particular included a 2016 advisory mission to consult with the cybercrime unit of the police, the digital forensic unit, the prosecutor for cybercrime cases, ARKEP and ISPs on reporting mechanisms for online fraud and other kind of cybercrime or cyber-enabled crimes;[110] a workshop in 2016 to further inter-agency and international cooperation and information-sharing between cybercrime units and supporting investigation units and the relevant authorities for judicial cooperation to facilitate the (cross-border) search and seizure of cybercrime proceeds;[111] a cybercrime simulation exercise in 2017 involving and testing domestic cooperation among cybercrime investigators, digital forensics experts, financial investigators, prosecutors and the financial intelligence unit;[112] and a live data forensics training conducted by the European Cybercrime Training and Education Group (ECTEG) in 2018—an intermediate-level course comprising theoretical and practical elements specifically geared towards strengthening the capacity of cybercrime investigators, digital forensics specialist and first responders.[113]

Based on responses from cybercrime investigators surveyed by iPROCEEDS, criminal investigations are conducted according to the KP's Standard Operating Procedures for the seizure of electronic evidence and international best practices, including the CoE`s Guidelines on Electronic Evidence.[114]

Under the framework of its Kosovo Safety and Security Programme, the UNDP in November 2018 launched a two-year project to facilitate Combating Cyber Crime in Kosovo (C3K).[115] Funded by the Norwegian Government, the project's efforts focus on five main areas of activity: (1) supporting the national CERT in improving incident reporting and communication

[110] iPROCEEDS Activity 1.3.5, Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms, Council of Europe, August 2016, https://rm.coe.int/3156-advisory-mission-reporting-kosovo-outline-web/16808c8c29.

[111] "iPROCEEDS: Inter-Agency and International Cooperation for Search, Seizure and Confiscation of Online Crime Proceeds," iPROCEEDS Activities, Council of Europe, 8 December 2016, https://www.coe.int/en/web/cybercrime/-/iproceeds-inter-agency-and-international-cooperation-for-search-seizure-and-confiscation-of-online-crime-proceeds.

[112] "iPROCEEDS: Cybercrime Simulation Exercise: Investigating cybercrime and its financial gain," iPROCEEDS Activities, Council of Europe, 16 November 2017, https://www.coe.int/en/web/cybercrime/-/iproceeds-cybercrime-simulation-exercise-investigating-cybercrime-and-its-financial-ga-2.

[113] "iPROCEEDS: ECTEG Live Data Forensics Training," iPROCEEDS Activities, Council of Europe, 13 July 2018, https://www.coe.int/en/web/cybercrime/-/iproceeds-ecteg-live-data-forensics-training.

[114] "Assessment report on obtaining and using electronic evidence in criminal proceedings under domestic legislation in South-eastern Europe and Turkey," iPROCEEDS, Council of Europe, March 2018, 38 https://rm.coe.int/0900001680931f06.

[115] "UNDP and the Royal Norwegian Embassy signed a new project agreement to support the security sector and access to justice," UNDP Kosovo, 7 November 2018, https://www.ks.undp.org/content/kosovo/en/home/presscenter/pressreleases/2018/11/undp-and-the-royal-norwegian-embassy-signed-a-new-project-agreem.html.

between the CERT and the cybercrime investigation unit of the KP; (2) setting up a security information and event management (SIEM) system for the KP to protect internal data bases; (3) enhancing digital forensics capabilities with a focus on mobile devices; (4) developing expertise for darknet investigations; and (5) supporting awareness campaigns for citizens and for institutions about their specific cyber risk profile and available assistance.

The *Strategic Plan of Prosecutorial System* [sic] for 2019–2021, prepared by the Kosovo Prosecutorial Council and the Office of the State Prosecutor, identifies the investigation of cybercrimes as a priority area and notes the need to increase the efficiency of criminal proceedings related to cybercrime.[116]

Judges and prosecutors are required to take part in annual professional trainings, which includes options on cybercrime. As part of its continuous training programme for judges and prosecutors, the Academy of Justice in early 2019 organised a training focused on the handling of electronic evidence in cybercrime investigations. Since 2016, the Academy has been conducting a specialised multi-session training programme to bolster capacity for combating cybercrime on an annual basis. No comparative programmes specifically focused on cybercrime have so far been offered for the initial training period of newly appointed judges and prosecutors. Initial training programmes, however, may touch on aspects related to cybercrime as part of their coverage of serious crimes.

To recruit junior professionals with a background in cybercrime investigations, the Ministry of Justice (MoJ) has invested in efforts to incentivise students specialising in cybercrime matters at prestigious universities abroad to return to Kosovo and join the MoJ after graduation.

Through their joint project, iPROCEEDS, the EU and the CoE have organised two training courses in 2018[117] and 2019[118] for judges and prosecutors from Kosovo. Conducted by local trainers with support from international experts, the trainings addressed current cybercrime trends, underlying technology, core aspects of cybercrime legislation, procedures and practice related to electronic evidence and mechanisms for international and public-private sector cooperation in the fight of cybercrime. Upon conclusion of the project, iPROCEEDS assessed that the established pool of national experts would be able to continue to deliver CoE training material within the framework of the Academy of Justice and could ensure sustainable training.

At least one judge and one prosecutor are offering training for trainers on cybercrime matters through the training programmes run by the Academy of Justice.

[116] Kosovo Prosecutorial Council and Office of the State Prosecutor of the Republic of Kosovo, Strategic Plan of Prosecutorial System 2019-2021, February 2019, http://kpk-rks.org/assets/cms/uploads/files/Statistika%20dhe%20Raporte/Strategic%20Plan%20of%20Prosecutorial%20System%202019%20-%202021.pdf.

[117] "iPROCEEDS: Introductory Judicial Course on Cybercrime, Electronic Evidence and Online Crime Proceeds," iPROCEEDS Activities, Council of Europe, 10 February 2018, https://www.coe.int/en/web/cybercrime/-/iproceeds-introductory-judicial-course-on-cybercrime-electronic-evidence-and-online-crime-procee-1.

[118] "iPROCEEDS: Supports the Second National Delivery of the Introductory Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds," iPROCEEDS Activities, Council of Europe, 22 February 2019, https://www.coe.int/en/web/cybercrime/-/iprocee-2.

International observers in the field of capacity building that were consulted for this assessment submitted that judges are currently left to take the reports of digital forensics experts at face value. Noting a lack of private digital forensic labs registered in Kosovo that could be contracted to challenge assessments presented by prosecutors, accused parties were unlikely to have expert witnesses at their disposal for a fair defence.

D4.2 Criminal Justice System (*referred to as "Legal Investigation" CMM Report Kosovo 2015*)

Areas of Capacity Advancements	**Areas of Consolidation**	**Enduring Challenges**
↑ Prosecutors and judges trained through international programmes in electronic incident handling and cross-border cooperation, including training of trainers initiatives	→ Forensic training of specialised cybercrime unit within the Kosovo Police	! Need for further clarification on the handling of electronic evidence in policy operating procedures ! Need for clear definitions of electronic evidence in the Criminal Procedure Code ! Limited availability of cybercrime training programmes for newly appointed judges and prosecutors

Maturity Levels in Comparison 2015 : 2019

2015 – Formative | **2019 – Formative to Established**

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

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

Stage: Formative to Established

The overarching *Law on International Legal Cooperation in Criminal Matters*,[119] which regulates mutual legal assistance, also extends to cooperation to combat cybercrime (Chapter VI). Provisions of this law also allow for the spontaneous exchange of information without a prior request for formal cooperation within conditions specified by the MoJ (Art.92). The *Law on the Prevention and Fight of Cybercrime* reaffirms these rules in their application to cybercrime matters (Art.20-22). The cybercrime law explicitly provides for international legal assistance for criminal proceedings, extradition, the identification, blocking and confiscation of products and means used in carrying out the criminal act, for carrying out investigations, the exchange and collection of information, and the request or provision of technical assistance and specialised training of personnel (Art.20).

Formal requests for legal cooperation are generally placed and processed on the basis of mutual legal assistance treaties (MLATs). The Department of International Legal Cooperation (DILC) within the MoJ serves as the central point of contact for mutual legal assistance in criminal matters. Kosovo has not yet set up a 24/7 point of contact. Requests for the police can, however, be submitted on an informal basis to the Directorate for International Cooperation in the Rule of Law of the KP. The Criminal Procedure Code requires state prosecutors and competent judges to consult and comply with the opinion of the DILC in filing requests for legal cooperation (Art.219.3). Final authority to approve cooperation requests to foreign governments rests with the MoJ (Art.219.4). Requests received by the DILC will be delegated to the appropriate state prosecutor (Criminal Procedure Code, Art.219.7; Law on International Legal Cooperation in Criminal Matters, Art.84).

Kosovo has signed MLATs with a range of neighbouring and EU countries, including North Macedonia, Albania, Germany, Italy and Hungary. In June 2019, the extradition treaty between Kosovo and the US came into force. Institutionalised channels provided through MLATs serve as essential means to secure and preserve transitory data of low shelf life in the effort to collect evidence. The MoJ has collated all agreements in central references and prepared commentary for all articles and provisions included in this resource. In support of requests for international legal cooperation, the MoJ has produced templates for submission to foreign governments. The DILC has also processed requests for cooperation even in the absence of a formal cooperation arrangement based on assurances of reciprocity.

[119] Law on International Legal Cooperation in Criminal Matters of 2013, no. 04/L-213, Official Gazette of the Republic of Kosovo 33/2013 https://gzk.rks-gov.net/ActDetail.aspx?ActID=8871.

The Republic of Kosovo enjoys good cooperation with countries that have not formally recognised Kosovo. Kosovo also complies with extradition requests submitted by these countries. It is worth noting, however, that with respect to at least one of these countries, extradition procedures have not yet been tested. Kosovo processes all requests for international legal cooperation with the above-mentioned countries based on the principle of reciprocity. Efforts to establish collaboration on this basis remain ongoing with one individual state that has not officially recognised Kosovo, including in the case of a suspect wanted for murder and searched based on an Interpol arrest warrant.

While primarily focused on issues related to the trafficking of human beings, arms and illicit drugs, the prosecutors' network of the Western Balkans for international cooperation in criminal justice[120] established by the EU Instrument for Pre-accession Assistance, could also provide a platform and institutional links to increase consultations on cybercrime. As mentioned above, prosecutors and judges in Kosovo have benefited from workshops and trainings on international legal cooperation as envisaged under the Budapest Convention that were organised within the framework of iPROCEEDS.

Assistance between Kosovo authorities and ISPs is widely codified. Production orders for subscriber information held by electronic service providers (Art.68) as well as the supervision and monitoring of electronic communications traffic (Art.104) are regulated by the *Law on Electronic Communications*. The *Law on the Prevention and Fight of the Cybercrime* addresses search and seizure of stored data and the real-time collection of data traffic for the purpose of securing electronic evidence (Art.18, 19). Where this is expected to produce important information for an investigation or identification of perpetrators cannot be achieved by other means, the *Law on the Prevention and Fight of the Cybercrime*, for strictly defined periods of time, allows prosecutors to order law enforcement to access a computer system for the purpose of intercepting or recording communications (Art.19). Kosovo's main ISPs are reported to have designated a data protection officer specifically to respond to law enforcement requests for access to customer data, and to act only on judicial authorisation. Compliance with these routines in the interactions between law enforcement and ISPs could not be independently verified at the time of this assessment given resource constraints at the NAPPD that limit the agency's capacity to conduct inspections.

[120] International Cooperation in Criminal Justice: Prosecutors' Network of The Western Balkans, accessed 1 November 2019, http://www.prosecutorsnetwork.org/.

RECOMMENDATIONS

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

LEGAL FRAMEWORKS

R4.1 Ensure that consultations for the new comprehensive cybersecurity law offer opportunity for all relevant stakeholders to provide input for consideration; invest in inclusive consultations to develop "buy-in" of critical stakeholders in the implementation phase of the law.

R4.2 If a new agency dedicated to cybersecurity is to be created under the new cybersecurity law, consider a decentralised approach (as exemplified by the model chosen for the UK National Cyber Security Centre): an integrated agency staffed by officials seconded from ministries and agencies already involved in certain aspects of cybersecurity; this approach may help increase coordination and can leverage existing resources to greater potential while keeping the existing distribution of responsibilities between ministries in place.

R4.3 If enacted separately, ensure that consultations for the new law on cybercrime offer opportunity for all relevant stakeholders to provide input for consideration; invest in inclusive consultations to develop "buy-in" of critical stakeholders in the implementation phase of the law.

R4.4 In anticipation of legislation transposing the EU NIS Directive, explore ways to effectively communicate to members of parliament which provisions in draft legislation are linked to the transposition of the EU *acquis* to ensure that these provisions are not deleted by mistake. (Other countries in the EU neighbourhood mark such provisions with the EU flag.)

R4.5. Support the selection of a non-political candidate as commissioner of the NAPPD; to this end, ensure that the selection panel tasked by the Parliamentary Committee for Security with the preparation of a shortlist of candidates is composed of data protection experts or professionals of associate fields.

R4.6 Facilitate the swift appointment of a commissioner to lead the NAPPD and the completion of the necessary legal steps for the agency to resume its inspections within the shortest delay possible.

R4.7 Ensure sufficient and appropriately qualified staffing for the NAPPD to carry out its inspection responsibilities.

R4.8 Conduct an assessment of the particular harms to which children in Kosovo are exposed online and in their use of connected devices and social media; develop specific measures to protect children from these harms.

R4.9 Evaluate the need for specific adaptions to consumer protection legislation to ensure that the same rights that apply offline also apply online.

R4.10 Evaluate the need for specific adaptions to legislation on intellectual property protection to ensure that the same rights that apply offline also apply online.

CRIMINAL JUSTICE SYSTEM

R4.11 Ensure that judges presiding over cybercrime cases are trained to recognise them as such and base their rulings on the full breadth of cybercrime legislation applicable in Kosovo, including the *Law on the Prevention and Fight of Cybercrime*.

R4.12 Review and update the Criminal Procedure Code with clear definitions of electronic evidence.

R4.13 Define and specify explicit procedures and practices for the handling of electronic evidence in standard operating procedures of the Kosovo Police.

R4.14 Train judges to adjust and limit the scope of data preservation orders to the specific requirements of the criminal investigation they support.

R4.15 Expand specific training on cybercrime to the initial training programmes of newly appointed judges and prosecutors.

R4.16 Ensure the general availability of independent digital forensics expertise that may be contracted by defendants in cases involving electronic evidence to enable them to challenge forensic assessments presented by prosecutors.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.17 Evaluate the efficiency and efficacy of arrangements for formal international legal cooperation in their application to the investigation and prosecution of cybercrimes; document and address any challenges identified.

R4.18 Develop reliable procedures for securing volatile, time-sensitive electronic evidence where international cooperation relationships require legal assistance requests to be submitted via circuitous diplomatic channels instead of a direct contact within the foreign government's competent authority.

R4.19 Explore possibilities to leverage the Prosecutors' Network in the Western Balkans as a platform to advance exchanges and collaboration on cybercrime.

R4.20 Facilitate a regular and independent evaluation of the interactions and cooperation between law enforcement and electronic service providers to ensure their compliance with legal standards.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

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

D 5.1 ADHERENCE TO STANDARDS

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

Stage: Formative

In 2015, consideration of international ICT security and risk management standards for many organisations had only reached an exploratory stage. Adoption proves selective and limited, with the private sector leading in adoption rates. This imbalance between private and public sector organisations in the uptake of international security frameworks remains noticeable in 2019. In a first step, standardisation efforts are occupied with developing policies and harmonising practices within the organisation. Only a subset of domestic organisations and local companies moves on to external guidance, mostly ISO resources, to improve on these internal practices.

In the view of consulted stakeholders, concerns about business reputation and its effects on corporate profits have acted as the main drivers pushing the adoption of internationally recognised security standards. In line with these concerns, adopted measures tend to focus on the protection of customer data. Measures of this kind seek to ensure formal compliance with the legal requirements for data protection, while placing less emphasis on the technical practicalities of the appropriate safeguards that underwrite any real security improvements.

The effective identification of critical infrastructure systems, once in place, could provide a platform to advance and develop sector-specific policies for the mandatory and monitored implementation of standards. Presently, Kosovo benefits from the fact that many of the larger private companies operating in Kosovo operate as subsidiaries of transnational companies and follow more advanced security requirements set in other jurisdictions. Their roots in foreign legislation nonetheless limit the vision of Kosovar authorities into how these practices are applied and actual compliance with them in Kosovo.

The uplift extended by international corporations likewise offers no remediation of the gap in standards adoption that exists between the public and the private sector. Public-sector organisations interviewed for this report expressed demand for programmes facilitating the exchange of experience in the implementation of security and risk-management standards between the public and private sector.

Following the 2015 CMM baseline assessment, in 2016 the telecom regulator ARKEP took the initiative and issued regulations specific to network and electronic-service providers based on authority conferred by the *Law on Electronic Communications*. Drawing on the EU Framework Directive 2009/140/EC[121] and technical guidelines on minimum security measures subsequently developed by the European Cybersecurity Agency ENISA,[122] inspired by the ISO 27000 series of standards, Regulation No. 29[123] establishes technical and organisational standards for security and integrity. Specifically, the regulation requires operators with annual revenue in excess of €500,000 to submit to regular independent security audits and to share the resulting reports with the overseeing authority, KOS-CERT, which operates under ARKEP. Paid for by the operators and scheduled to be conducted every two years, the first round of audits has been submitted to KOS-CERT, showing moderate levels of implementation of the identified minimum technical security measures.[124]

The 2011 *Law on Public Procurement*[125] remained the authoritative source delineating spending criteria for public funds in 2019. Amendments to the law enacted since 2011 and after the baseline CMM in 2015 have not materially changed the regulatory landscape with respect to the consideration given to ICT security standards. The *National Strategy on Public*

[121] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, Official Journal of the European Union L 337/37, http://data.europa.eu/eli/dir/2009/140/oj.

[122] ENISA, "Incident Reporting for Telcos," accessed 1 November 2019, https://www.enisa.europa.eu/topics/incident-reporting/for-telcos.

[123] ARKEP, Regulation on Technical and Organisational Standards for Security and Integrity of Electronic Communication Networks and/or Services of 2016*,* Prot. No. 046/B/16, https://www.arkep-rks.org/?cid=1,34,953.

[124] Annex 3 on *Minimal Technical Measures for Security and Integrity of Electronic Communication Networks and/or Services* of the *Regulation on Technical and Organisational Standards for Security and Integrity of Electronic Communication Networks and/or Services*.

[125] Law on Public Procurement in the Republic of Kosovo of 2011, no. 04/L-042, Official Gazette of the Republic of Kosovo 18/2011, https://gzk.rks-gov.net/ActDetail.aspx?ActID=2772.

Procurement 2017–2021, developed by the independent Public Procurement Regulatory Commission (PPRC) which oversees public procurement procedures, similarly contains no direct mention of the role of ICT security in procurement decisions. While the Strategy introduces new socio-economic and environmental objectives as assessment criteria and emphasises the potential of IT for enhancing the efficiency and transparency of public procurement processes, the planning document not address the need for securing these technologies and systems when they become the subject of procurement.[126]

The closest to a reference to technology security standards in the *Law on Public Procurement* is the option to review bids based on their "technical merits" (Art.52.3), which is different still from legal requirements to make the consideration of ICT security standards an integral part of tender specifications. Under the law, any such review of technical merits has to maintain technology neutrality. Article 28.2, addressing the technical specifications of public tenders, could in principle allow for the inclusion of security criteria on the condition that these prove "consistent with the purpose of the procurement", provided that they remain directed at ensuring "the greatest possible access to all potentially interested economic operators and tenderers". Contract award criteria set out in Art.60.1.1.2 provide for the selection of the "most economically advantageous" bid, as defined against the tender's technical specification. Consideration of ICT security aspects thus depends on the priority assigned to it by individual procurement and authorising officers. Officers in this capacity may operate without the necessary budget line to make the inclusion of security criteria a feasible proposition. Civil servants involved in public procurement procedures consulted for this assessment reported often lengthy decision-making processes that at their conclusion are primarily decided by cost considerations in which the lowest-cost option wins out, even as professional staff raised the importance of security criteria. Interviewed participants voiced concern that this price-driven decision-making opens Kosovo up to strategic dumping by neighbours with the intention to place subsidised systems in Kosovo's infrastructure ecosystem and government networks. Aside from possible security risks, this practice would award public funds to foreign companies for lucrative follow-up contracts to ensure maintenance of the supplied software and equipment.

Large-scale infrastructure modernisation projects currently in planning, including upgrades to the railway signalling system, are bound to have systemic effects on the public security posture. These projects offer an opportunity to include ICT security considerations by design and make them one of the central concerns when replacing legacy systems. ARKEP has been leading the way for the network and electronic service providers it oversees. ARKEP regulations require operators to develop security policies for contacts signed with third parties that need to be followed in procurement decisions. These policies are to address the "explicit security requirements in the contracts with third parties supplying IT products, IT services,

[126] Public Procurement Regulatory Commission, National Public Procurement Strategy 2017-2021, January 2017, https://krpp.rks-gov.net/krpp/PageFiles/File/Objektivat%20e%20Krpp%20se/2017/Strategy%20for%20Public%20Procurement%202017.pdf.

outsourced business processes, helpdesks, call centres, interconnections, shared facilities, etc.”[127]

Since 2016, public procurement requests can be managed through an online platform run by the PPRC, which has been established with support from World Bank-funded Public Sector Modernization Project. Use of this e-procurement system has been phased in as a mandatory practice. As of May 2018, 97 percent of cases were handled digitally, increasing access and participation of SMEs in the bidding competitions.[128]

With regard to software development, no coherent approach or well-defined frameworks are being promoted by government. This situation, as in 2015, results in the majority of software development needs being contracted out. In practice, the software development methodologies applied consider integrity and resilience in as much as they are embedded in external APIs that often form the foundation of many projects.

Within the Government of Kosovo, an overwhelming share of software-development initiatives rely on global solutions for development platform technologies. In the private sector, many companies offering software-development services work with Agile software-development methods.

D5.1 Adherence to Standards

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ Compliance efforts with legal requirements for data protection ↑ Minimum technical standards specified for one sector based on ENISA and ISO guidance ↑ Minimum technical standards audited for one select sector	→ Integration of integrity and resilience principles into software development due to reliance on third-party APIs	! With the exception of electronic service providers, no specific ICT security requirements for *de facto* CNI operators ! Technology security not viewed as integral part of procurement decisions

Maturity Levels in Comparison 2015 : 2019

2015 – Formative | 2019 – Formative

[127] Annex 3 on *Minimal Technical Measures for Security and Integrity of Electronic Communication Networks and/or Services* of the *Regulation on Technical and Organisational Standards for Security and Integrity of Electronic Communication Networks and/or Services*.

[128] Public Procurement Regulatory Commission, “E-Procurement in Kosovo,” 10 May 2018, 45, http://pubdocs.worldbank.org/en/499511525762426135/En-KOSOVO-E-Procurement.pdf.

D 5.2 INTERNET INFRASTRUCTURE RESILIENCE

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

Stage: Formative

Based on the latest Annual Report of ARKEP, issued for the year 2017, 76% of households had fixed-line access to broadband Internet.[129] On a per-capita basis, penetration rates, however, lie significantly below these levels, dropping to 15.1%. Both metrics have increased since 2015, when household access stood at 73.1% and access rates for individual users reached 11.9%. For 2018 and 2019, Eurostat reports a markedly higher rate of broadband access, extending to 93% of households.[130] Since mobile Internet was first introduced in December 2013, subscriptions have risen sharply,[131] resulting in a mobile Internet access rate (3G+4G) of 92% in 2018.[132]

Three main ISPs connect users and businesses in Kosovo to international Internet gateways: IPKO (market share of 47% of Internet end-users), Kujtesa (25%) and Kosovo Telecom (previously Post and Telecommunications of Kosovo; 16%).[133] The remaining market (12%) is shared by 51 smaller regional operators[134] that mainly provide connectivity for the last mile. According to a World Bank survey of 2017, just about 1% of households had access to fibre optic-based Internet connection (over 100Mbps).[135] Notable regional divides exist with regard to fixed broadband penetration. In particular, districts in the south-west and the north of Kosovo have penetration rates that fall between 30 and 40 percentage points below the national average.[136]

To address these disparities, in 2018 the World Bank approved the Kosovo Digital Economy (KODE) project with the goal to improve access to better quality and high-speed broadband services in project areas and to online knowledge sources, services and labour markets among citizens, and public and academic institutions. The project is set to offer connectivity to schools and hospitals in Project areas for five years, free of charge.[137] The same project also

[129] ARKEP, "Annual Report 2017," 2017, https://www.arkep-rks.org/?cid=1,32,1142.

[130] Eurostat, "Households with Broadband Access," last updated 29 January 2020, https://ec.europa.eu/eurostat/databrowser/view/tin00073/default/table?lang=en.

[131] World Bank, Kosovo Digital Economy (KODE) Project, Project Appraisal Document 613, 2018, 45, http://documents.worldbank.org/curated/en/249951531020771941/pdf/Kosovo-KODE-PAD-06132018.pdf.

[132] TeleGeography, GlobalComms: Eastern Europe Database, https://www2.telegeography.com

[133] ARKEP, "Annual Report 2017," 2017, https://www.arkep-rks.org/?cid=1,32,1142.

[134] Kosovo Digital Economy (KODE)project, Project Appraisal Document 613, 70.

[135] Ibid., 12.

[136] Ibid., 72.

[137] World Bank, Project Appraisal Document on a Proposed Credit to the Republic of Kosovo for a Kosovo Digital Economy (KODE) Project, Report no. PAD2669, 31 May 2018,

seeks to connect colleges and universities in Kosovo to the GÉANT network that links national research and education networking organisations. Kosovo, at present, works to establish its own national research and education network (NREN).

ISPs are obliged to provide information on the equipment they deploy to ARKEP. For the past years, these obligations have been observed for telephone landlines and mobile networks. In 2019, these rules, for the first time, have been applied to infrastructure supporting fixed Internet connections. In addition, ISPs are required to conduct impact assessments of any incidents occurring on their networks based on a framework provided by ARKEP as part of the 2016 Regulation on Technical and Organisational Standards. Any incident assessed to be of medium or high impact needs to be reported to KOS-CERT without delay.

According to reporting collected by KOS-CERT, no major outage of serious consequence has been recorded, only isolated incidents. Detection and reporting of malicious network activity that could pose risks to Internet infrastructure resilience, however, is complicated by the fact that the IP address space in Kosovo is not yet defined. Most of Kosovo's ISPs are registered as Albanian or Serbian, as Kosovo is not officially represented in any regional Internet registry. This means that some reports for incidents originating in Kosovo may be reported to Albanian authorities, who commonly forward reports to Kosovo. This referral practice, however, does not provide for a systematic or timely way to review incident reports. Some of the participants consulted for this report further cautioned that the same forwarding practice is not always applied with the same routine in cases where external incident reports concerning IP addresses located in Kosovo are submitted to Serbian authorities.

D5.2 Internet Infrastructure Resilience

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ Rollout of high-speed mobile Internet diversifying Internet access options		! Regional divides in Internet penetration ! Limited control over national IP address space due to lack of representation in Internet infrastructure governance

Maturity Levels in Comparison 2015 : 2019

2015 – Formative

2019 – Formative

https://www.worldbank.org/en/news/feature/2018/11/26/kosovo-villages-start-enjoying-high-speed-internet-with-world-bank-support.

D 5.3 SOFTWARE QUALITY

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

Stage: Formative

Based on a 2018 survey of 36 IT companies operating in Kosovo, conducted by the Kosovo Association of Information and Communication Technology (STIKK), only half of the firms consulted have pursued any form of quality certification[138] for their products.[139] The primary motivation cited by companies that had undergone certification against quality management standards was to improve processes within the company; only 12 percent reported to have pursued quality management standards in response to or in anticipation of client requests. Less than half of the IT firms surveyed stated that they had been approached by clients with any requests to provide certified quality assurance. These findings are anecdotally supported by responses collected during the consultations for this assessment. Participants interviewed described customer evaluation of software quality as primarily driven by price considerations.

Kosovo's major ISPs have developed and implement policies for patch management and for maintaining systems under their supervision. These policies have been extended to include third-party suppliers. For many other businesses, however, especially outside of the ICT security market, systematic checks for and application of security updates are not a high priority in light of resource constraints. Widespread use of pirated software fundamentally limits access to security updates.

Patch management and maintenance often appears to be tied to framework updates. Updates introducing a new software version with added functionality, reportedly, fetch higher rates of implementation, albeit not in all instances out of an appreciation or assessment of the potential security concerns related to running outdated programmes. These practices indicate that a logical issue discovered in the software might go unfixed for an extended period of time.

Noting the exception of start-ups that are focused on functionality under pressure to move their software solutions to market, participants observed that software firms catering to the private sector assigned greater importance to quality control in their engineering. This may be due to the export orientation of many IT firms operating in Kosovo and the influence of quality requirements introduced by international business considerations. Of the 36 companies surveyed by STIKK, 44 percent named customers abroad as their primary market,

[138] Companies were surveyed on a range of quality standards, including on general quality management and information security, with the opportunity to provide alternative responses. A relative majority of most positive responses identified ISO 9001 on quality management (36%). The application of ISO 9001 principles to computer software as evaluated by ISO 90003 was not explicitly surveyed.

[139] STIKK, "Kosovo IT Barometer 2018," November 2018, 17, https://stikk.org/wp-content/uploads/2018/12/Publications_2018_-_IT_Barometer_EN.pdf.

with an additional 14 percent ascribing equal importance to domestic and export markets.[140] Even on the domestic market, 61 percent of the companies reported providing services to international organisations and clients based in Kosovo.[141]

For software developed within government, the AIS within the Ministry of Public Administration is mandated to inspect the source code and red-team any new solution before the application can be approved for use.

D 5.4 TECHNICAL SECURITY CONTROLS

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

Stage: Formative

Based on a comparative review of industry practices conducted by local university research, financial institutions are leading nationally in the adoption of technical security controls and follow global standards to maintain international business and access to banking networks. These security measures extend to physical access controls for sensitive computing facilities. According to the study, banks and insurance companies run own internal servers for their business operations and distribute backups across multiple data centres.

Software-development companies were found to implement network-security measures to facilitate the early detection of intrusions, but appeared to be lacking in strategic planning for data backups, which could potentially open firms up to risks of data corruption. A vast majority of these firms reportedly uses internal servers for storing work products and development tools, while relying on external server infrastructure for email services and cloud solutions as a data-backup option.

KOS-CERT, which has received the first instalment of security audits from ISPs, assessed that ISPs on the whole marshal the technical and human capacity to put appropriate security controls in place, supported by a backup policy. Assessments of the security measures undertaken in other sectors carried markedly less confidence due to the limited visibility into their practices.

ISPs reported requests from clients for “pure Internet” without any upstream filtering of traffic on the part of providers. In response to these requests, some ISPs have switched to providing optional filter packages for known malware, pornographic content and customised solutions for educational institutions that, for instance, restrict access to social media platforms. Major ISPs, however, have maintained upstream filtering of malicious content and offer additional security services including protection against denial-of-service attacks.

[140] “Kosovo IT Barometer 2018,” 18.

[141] “Kosovo IT Barometer 2018,” 20.

Public organisations that seek to make software solutions accessible to other agencies or lack the resources to secure sensitive data can make use of hosting facilities that the AIS operates as part of the government data centre. The AIS, however, does not run a disaster recovery centre. Kosovo's limited geography (in terms of Kosovo's north-south and east-west expanse and its topographic diversity) may pose challenges for complying with best practices intended to shield data hubs from natural or man-made disasters, such as requirements for a minimum distance between secondary data recovery centres and the main facility.

In December 2018, the email system of the Ministry of Foreign Affairs became the target of attacks with the presumed intention of disrupting electronic communications between the Government in Pristina and its international diplomatic representation.[142] Managed by the AIS, which oversees the security and protection of electronic communication infrastructure of government institutions, the incident serves as important reminder to ensure the availability of tested redundancy and recovery mechanisms.

D 5.5 CRYPTOGRAPHIC CONTROLS

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

Stage: Start-up

Kosovo's larger ISPs and telecommunication companies encrypt sensitive data at rest and manage employee access on a restrictive need-to-know basis. Awareness training on technical data protection measures and applicable corporate policies has purportedly facilitated active reporting by employees in instances where these policies have broken down and access protocols have not been fully implemented.

At least one major software-development and engineering company consulted for this assessment reported a general absence of cryptographic requirements in their contract work, citing only one project over the span of the last 12 years that stipulated special cryptographic needs. Software companies raised political obstacles related to questions of Kosovo's international recognition that were seen as impeding access to certain technology imports, noting that not all international vendors of choice offered to license encryption solutions for use in Kosovo. To the knowledge of the participants interviewed, none of the research centres at universities in Kosovo focuses on developing bridging encryption solutions.

[142] "Veliki sajber napad Srbije na Kosovu: Hakovane ključne institucije," *Kosovo Server portal*, 7 December 2018, https://kossev.info/veliki-sajber-napad-na-kosovu-hakovane-kljucne-institucije/; "Government reports cyber attack on Kosovo institutions," *N1*, 7 December 2018, https://rs.n1info.com/English/NEWS/a442278/Government-reports-cyber-attack-on-Kosovo-institutions.html.

With respect to user behaviour, private-sector representatives assessed that older generations, while used to prolific practices of surveillance by analogue means in the past, did not generally apply the same precautious mind-set in their use of networked devices or online services. Younger generations, by comparison, showed greater appreciation of the privacy and data protection concerns linked to online activity, though participants were less confident about how effectively this understanding translated to the use of appropriate protection such as the use of messengers supporting end-to-end encryption.

The Government of Kosovo is implementing a bespoke public-key infrastructure (PKI) arrangement for government backbone networks.

D 5.6 CYBERSECURITY MARKETPLACE

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

Stage: Start-up

As noted above, IT firms in Kosovo share a strong export orientation, with close to half naming overseas markets as their primary customer base. For companies driving innovation in Kosovo, this strong export focus is even more pronounced, with up to 90 percent of their revenue relying on overseas markets. Many of these companies operate offices or joint ventures in the USA and Germany.

Conversely, most solutions and products in use in Kosovo are imported. National security exceptions exist for certain hardware components, however, including network switches which, by law, are not allowed to be sourced from vendors based in China and Russia. Yet these exceptions are not expressly codified and implemented based on a *de facto* assessment. As assessed in 2015, the limited size of the domestic technology ecosystem only offers restricted potential to scale up for local companies, leading them to seek out more profitable margins abroad. Several companies offer penetration-testing services domestically. Private-sector representatives signalled demand for a platform linking start-ups and other local providers to potential domestic customers. Larger companies with in-house software engineering expertise on occasion draw on open-source products and adapt them to custom requirements, citing concerns that household-name products may be more likely to become the target of malicious actors unless supported with a sufficiently staffed and resourced security team.

As observed in 2015, the identification of the need for cybersecurity insurance remains largely confined to banks and concerns related to losses due to data breaches. Representatives from other industries in the private sector stated that they were not aware of any cybersecurity insurance offerings that catered specifically to the market in Kosovo. The same group conjectured that such offerings might prove “a losing battle” for insurance firms, suspecting that high premiums would limit uptake. Larger companies typically hold comprehensive third-party liability insurance packages and industrial fire insurance policies that, while not specific to cybersecurity risks, could mitigate damages resulting from inappropriate handling of data or physical hazards, e.g. in case of a data centre burning down.

D5.6 Cybersecurity Marketplace

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
↑ Exploratory analysis of supply chain security risks	→ Use of insurance against damages from cybercrime in the financial sector → Energetic backbone of IT security firms with international connections	! Supporting domestic innovation with market opportunities in Kosovo ! Evaluating the use of specific insurance policies to mitigate cyber-enabled risks

Maturity Levels in Comparison 2015 : 2019

2015 – Start-up | 2019 – Start-up

D 5.7 RESPONSIBLE DISCLOSURE

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

Stage: Start-up

Currently no frameworks or institutionalised channels exist for the responsible disclosure of security flaws to government agencies. Initiatives from the ethical hacker community to reach out to the Government, to establish such channels and a legal foundation to support the safe research and reporting of technical vulnerabilities to vendors and operators, have not been taken up.

Representatives of the private sector consulted saw raising awareness within Government about the security benefits of distributed vulnerability research—protecting users and companies faster and more reliably—as a gateway to obtaining political support for setting up a responsible disclosure mechanism.

In the past, researchers reaching out to ISPs with vulnerability information have been reported to the police by the companies notified. Security researchers expressed hopes that provisions on ethical hacking would form part of the comprehensive cybersecurity legislation currently under development. In the absence on specific legislation, the UNDP has organised training to offer guidance to ethical hackers.

Faced with circumstances of legal uncertainty, none of the companies consulted for this assessment felt in a position so set up a mechanism for responsible disclosure or could identify an entity with such a framework in place. One major e-commerce platform was reported to be setting up a bug bounty programme.

D5.7 Responsible Disclosure (*assessed in D4.3 in CMM Report Kosovo 2015*)

Areas of Capacity Advancements	Areas of Consolidation	Enduring Challenges
	→ Strong sense of need for responsible disclosure frameworks among IT security firms	! Lack of legal basis for responsible vulnerability research and reporting ! Incentivising companies to set up formal channels to receive and address vulnerability information ! Mechanisms for information sharing within sectors

Maturity Levels in Comparison 2015 : 2019

2015 – Start-up	2019 – Start-up

RECOMMENDATIONS

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

ADHERENCE TO STANDARDS

R5.1 Leverage the presence of subsidiaries of international companies for public-private experience sharing on ICT standard adoption to close gap between public- and private-sector organisations.

R5.2 Ensure that the effective identification of critical infrastructure systems, once in place, can provide a platform to advance and outline sector-specific policies for the mandatory and monitored implementation of robust ICT security standards.

R5.3 Establish ICT security criteria as an integral part of procurement decisions involving software or information systems and technology.

R5.4 Address the integration of ICT security criteria into public tenders during procurement training offered by the Public Procurement Regulatory Commission.

R5.5 Set up government programmes to promote standards for software development that emphasise integrity and resilience, and monitor their adoption.

R5.6 Ensure that software development works actively towards integrity and resilience and does not depend on coincidental support from external APIs that may or may not deliberately address these objectives.

INTERNET INFRASTRUCTURE RESILIENCE

R5.7 Ensure that the available budget for national broadband development is also used to support and train smaller rural providers in security aspects; doing so within the scope of a national project offers advantages of economies of scale for training smaller providers.

R5.8 Make sure that the bulk of smaller providers have documented crisis response plans and defined roles and responsibilities to support the redundancy of national infrastructure.

SOFTWARE QUALITY

R5.9 Task government agencies to systematically collect evidence of quality deficiencies in the software that they deploy and assess their impact on usability and performance.

R5.10 Classify software applications for use by government agencies based on their reliability, usability and performance in adherence to international standards and good practices.

R5.11 Ensure that any existing vendor relationships do not constrain the choice of secure software platforms and applications.

TECHNICAL SECURITY CONTROLS

R5.12 Promote the adoption of up-to-date security controls, including network intrusion detection, regular data backups and consistent patch management, in the wider economy.

R5.13 Follow up on CNI identification with specific technical security controls for the respective sectors (following the example of ARKEP for ISPs).

R5.14 Collaborate with ISPs to raise awareness among end users about the importance of anti-malware software and network firewalls across devices.

R5.15 Establish a disaster recovery centre for the government data centre at as great a distance and topographical diversity from the main facility as geography allows.

CRYPTOGRAPHIC CONTROLS

R5.16 Where custom encryption solutions are cost-prohibitive, promote the use of off-the-shelf technology that also offers protection to data in transit through end-to-end encryption.

R5.17 Raise awareness about the importance of encrypting data in transit and data at rest; incentivise its adoption throughout all sectors, especially by operators likely to receive designation as part of CNI.

R5.18 Explore how existing efforts for the integration of Kosovo into international technology markets (such as those organised through Digital Kosovo) can be leveraged to ensure access to preferred encryption solutions from international vendors.

CYBERSECURITY MARKETPLACE

R5.19 In consultation with the industry, consider establishing a platform for linking start-ups and other local providers to potential domestic customers.

R5.20 Promote the rigorous assessment of cybersecurity risks in the private sector and active consideration of the mitigation potential offered by cyber-insurance.

RESPONSIBLE DISCLOSURE

R5.21 Establish a legal basis for responsible vulnerability research and reporting; explore opportunities for introducing such provisions regulating safe ethical hacking as part of the comprehensive cybersecurity legislation currently under development.

R5.22 Incentivise companies to set up formal channels to receive and address vulnerability information related to their products.

R5.23 Support the creation of platforms and channels to facilitate the sharing of threat and vulnerability information at scale; ensure that information-sharing platforms are set up for the sectors identified as part of CNI.

ADDITIONAL REFLECTIONS

Consultations for the 2019 assessment notably expanded participation compared to 2015, including stakeholders from the private sector, from international partners, parliamentary committees, as well as from civil society organisations outside of the formal education sector. In addition, consultations in 2019 convened a number of stakeholders that had been interviewed in 2015, to track their views on capacity developments. Overall, more than 10 percent of stakeholders consulted for the 2019 assessment had also been interviewed in 2015. The 2019 review showed lower participation rates for the financial sector as commercial banks were collectively represented by the Kosovo Bank Banking Association.

While representatives of the MEST were not able to attend the review, the ministry holds significant responsibility for shaping cybersecurity awareness and ICT proficiency, especially among Kosovo's young population—around 38 percent of Kosovo's population are under the age of 20.[143] Kosovo's shortage of ICT and ICT security-specific professionals give MEST a central role in improving national conditions for talent development and establishing programmes that leverage a technology-trained population for socioeconomic development. Given the MED's responsibility in overseeing Kosovo's *IT Strategy*, including its components on workforce development, stakeholder input indicated the need for close coordination between the MEST and the MED in this endeavour, to ensure that curricula meet private-sector needs and provide for education that translates into employment.

To ensure that the assessment report can reflect the views of all key stakeholders that had been invited to the consultations, the GCSCC team has sought to provide additional opportunity for stakeholders that were unable to participate in person to provide comments and institutional perspectives in writing. Additional engagement efforts of this kind have been undertaken to receive input from representatives of the MIA that were not able to join the consultations conducted in Kosovo.

MIA participation in this MED-facilitated assessment is an essential precondition to help ensure that any recommendations provided by the GCSCC are targeted and reflective of the needs of the Government of Kosovo overall, so that the assessment report can facilitate further cooperation domestically as well as between Kosovo and its international partners. As described in detail in the body of this report, close coordination and a cooperative relationship between the MIA and MED are key to coherent capacity development given their respective responsibilities for legislation and strategic planning that critically shape Kosovo's cybersecurity posture.

To date, the GCSCC and its implementation partners have conducted CMM assessments across nearly 80 states, worldwide. The CMM has been deployed over a hundred times.

[143] "Republic of Kosovo Systematic Country Diagnostic," the World Bank Group, accessed 15 November 2019, http://documents.worldbank.org/curated/en/282091494340650708/pdf/Kosovo-SCD-FINAL-May-5-C-05052017.pdf

The CMM review of Kosovo informing this report was conducted in cooperation with the World Bank Group. Dissemination of the assessment report is organised in cooperation with the Global Cybersecurity Center for Development (GCCD) under the Korea Internet Security Agency (KISA) of Republic of Korea. Financing for this assessment has been provided by the Korea-World Bank Group Partnership Facility (KWPF) that is administered by the World Bank for South Korea's Ministry of Strategy and Finance.

Global Cyber Security Capacity Centre

Department of Computer Science, University of Oxford

Wolfson Building, Oxford OX1 3QD,

United Kingdom

Tel: +44 (0)1865 287434

Email: cybercapacity@cs.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk/cyber-security

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