National Cyber Security Strategy 2023-2027

September 2023

Table of content

1. LIST OF ABBREVIATIONS AND DEFINITIONS

1.1. Abbreviations

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
NCI	National Critical Infrastructure
CII	Critical Information Infrastructure
CSA	Cyber Security Agency
CSBM	Confidence and Security Building Measures
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECHR	European Court of Human Rights
ENISA	European Network and Information Security Agency
EU	European Union
EUROPOL	European Police Office
GoK	Government of Kosovo
ICT	Information and Communication Technology
INTERPOL	International Criminal Police Organization
IOCTA	Internet Organized Crime Threat Assessment
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
KP	Kosovo Police
LDCA	Live Distant Child Abuse
MIA	Ministry of Internal Affairs
NCSC	National Cyber Security Council
NFRT	National Flash Reaction Team
NIS Directive	The EU Network and Information Security Directive
OECD	Organization for Economic Cooperation and Development
OES	Operators of Essential Services
OPM	Office of the Prime Minister
PPP	Public Private Partnership
SGEM	Self-Generated Explicit Material
TLD	Top Level Domain
TOR	The Onion Router
UNDP	United Nations Development Programme
OSCE	Organization for Security and Cooperation in Europe
NATO	The North Atlantic Treaty Organization
GGE	Group of Governmental Experts of United Nations

1.2. Definitions

The following list includes many of the most common terms used in defining, describing, and exploring cyber security and related issues in the context of this document. The list should be used for reference but does not replace the definitions and descriptions set out in the legislation and strategies adopted.

1.2.1. Bug-Bounty

Means search for software vulnerabilities conducted by people not associated with the software developer, usually with the general consent of the developer.

1.2.2. Vital societal function

Means the activities, goods and services that are the basis for the general functioning of society.

1.2.3. Critical infrastructure

Means infrastructure, including facilities, systems, processes, networks, technologies, assets, and services - necessary to maintain or restore vital societal functions.

1.2.4. Critical ICT infrastructure

Means the subset of critical infrastructure that includes the digital infrastructure needed to maintain or restore vital societal functions.

1.2.5. National Critical Infrastructure

Means an asset, system or part thereof, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and disruption or destruction of which would have a significant impact on the Republic of Kosovo.

1.2.6. ICT systems critical to society

Means ICT systems where major disruptions result in significant challenges for society as a whole. The unavailability and unstable operation of ICT systems can have significant consequences for society and for the maintenance of processes critical to society.

1.2.7. Critical Information Infrastructure (CII)

a) An entity that provides a service which is essential for the maintenance of critical societal and/or economic activities, and
b) The provision of that service depends on network and information systems
c) An incident would have significant disruptive effects on the provision of that service.

1.2.8. Cyber Security

Means necessary activities to protect network and information systems, users of such systems and other persons affected by a cyber-incident;

1.2.9. Cybercrime

Means criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data.

1.2.10. Computer system

Means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

1.2.11. Computer data

Means the presentation of facts, information or concepts in a form suitable for processing in an information system, including a suitable program that causes an information system to perform a function. Computer data includes, but is not limited to written documents, pictures, audio and video materials, software programs and other digitally stored materials;

1.2.12. Data breach

Means the unauthorized disclosure of information that compromises the security, confidentiality, or integrity of personally identifiable information.

1.2.13. Distributed Denial-of-Service (DDoS)

Means a type of denial of service attack in which an attacker uses a malicious code installed on various computers to attack a single target.

1.2.14. Interdependency

Means the total or partial mutual dependency of several goods or services.

1.2.15. IT security

Ensures the availability, integrity, verifiability and confidentiality of information in the use of information technology. For this purpose,

- ‘Availability’ means the situation in which the necessary usability of information as IT systems and components is ensured;
- ‘Integrity’ refers to the exclusion of unauthorized and prohibited modifications of information as of IT systems and components;
- ‘Verifiability’ means the situation in which required or promised properties or features of information or transfer facilities can be verified by the users and vis-a-vis third parties;

- ‘Confidentiality’ refers to the exclusion of unauthorized obtaining or procuring of information.

1.2.16. Resilience

Means the ability to **prevent, resist, mitigate, absorb, accommodate and recover** from an incident that disrupts or has the potential to disrupt the operations of a critical entity.

1.2.17. Essential service

(a) a service which is essential for the maintenance of critical societal and/or economic activities.
(b) the provision of that service depends on network and information systems; and
(c) an incident would have significant disruptive effects on the provision of that service.

1.2.18. Hacker

Means someone who uses computers and the Internet to access computers and servers without permission.

1.2.19. Malicious Software or Malware

Means malicious software designed to infiltrate or damage a computer system without the owner’s consent. Common forms of *Malware* include computer viruses, worms, Trojans, spyware, adware, etc.

1.2.20. Ransomware

Means software that denies you access to your files until you pay a ransom.

1.2.21. Spear Phishing

Means the use of fraudulent emails to persuade people within an organization to reveal their usernames and/or passwords. Unlike phishing, which involves mass mailing, spear phishing is small-scaled and well targeted.

1.2.22. Service provider

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

1.2.23. Traffic data

Means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

1.2.24. Information system

Means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data, as well as computer data stored, processed, received or transmitted by such device or group of devices for the purposes of their operation, use, protection and maintenance;

1.2.25. Electronic communication network

Means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

1.2.26. Network and information system

1.2.26.1. An electronic communication network, as defined in paragraph 1.2.25;

1.2.26.2. any information system, as defined in paragraph 1.2.24;

1.2.26.3. digital data stored, processed, received or transmitted by elements covered in paragraphs 1.2.26.1. and 1.2.26.2. for the purposes of their operation, use, protection and maintenance;

1.2.27. Security of Network and information systems

Means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

1.2.28. Operator of essential services

is an entity fulfilling the following criteria:

- The entity provides a service which is essential for the maintenance of critical societal and/or economic activities.
- The provision of that service depends on network and information systems; and
- An incident would have significant disruptive effects on the provision of that service.

1.2.29. Digital service provider

Means any legal person that provides a digital service.

1.2.30. Internet Exchange Point (IXP)

Means a network facility which enables the interconnection of more than two independent autonomous systems. Local ISPs connect to IXP to exchange traffic instead of using upstream provider.

1.2.31. Domain Name System (*DNS*)

Means a hierarchical distributed naming system in a network which refers queries for domain names.

1.2.32. DNS service provider

Means an entity which provides DNS services on the internet.

1.2.33. Top-Level Domain(TLD)

Means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD).

***1.2.34. Online* marketplace**

Means a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.

1.2.35. Consumer

Means any natural person acting for purposes beyond his/her trade, business, craft or profession;

1.2.36. Trader

Means any natural person or legal entity, regardless of whether it is privately or publicly owned, who acts, including any person who acts for his/her account or on his/her behalf, for purposes related to his/her trade, business, craft or profession;

1.2.37. Online search engine

Means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language based on a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.

1.2.38. Cloud computing service

Means a digital service that enables access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services.

1.2.39. Internet of Things (*IoT*)

Means a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

1.2.40. Smart City

Means a designation given to a city that incorporates information and communication technologies (ICT) to enhance the quality and performance of urban services such as energy, transportation, and utilities in order to reduce resource consumption, wastage and overall costs.

2. INTRODUCTION

The National Cyber Security Strategy of the Republic of Kosovo presents a plan of directions, approaches, and strategic objectives approved by the Government of Kosovo aiming to improve the security and resilience of national infrastructures and services. The strategy document helps establish an approach to cyber security rooted in national objectives and priorities that should be achieved in a specific timeframe.

In Kosovo, the use of information and communication technology (ICT) has expanded rapidly since 2000, and ICT now plays an important role in all aspects of our lives. According to Internet World Stats, Internet penetration in Kosovo is 90.4% with 1,693,942 Internet users[1]. This trend of Internet distribution and use of ICT equipment is comparable to developed countries of the European Union, while the behavior of Kosovo citizens on the Internet seems to be similar to global trends. Most of Kosovo's institutions have moved their daily work online, including organizations providing services in critical infrastructure sectors such as energy, water, health, transport and communication. These systems improve the quality and speed of the services provided, helping organizations to work more productively, and contributing towards improving living standards.

Repeated analyzes show that the lives of Kosovars are largely reliant upon what we can now call traditional, but also emergent technologies, ensuring everyday crucial exchanges such as social communication, transactions with the private sector, academic endeavors and perhaps most relevant - exchanges with the public sector in receiving public services. For example, a Digital Household Survey conducted by UNDP Kosovo in 2021 with 2,400 households on access, use and affordability of digital tools, services related to behavior change, delivery of public services, etc., reveals that Kosovo has **wide** Internet **access** and ownership of Information and Communication Technology (ICT) devices such as computers and mobile phones among the population, with over **99.7% of the households** reported to **have access to the internet**[2].

Concurrently, a secure cyberspace is vital for the development of ICT and Internet services. In turn, the demand for internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings without due consideration for security. In addition, we see its applications in the provision of public services, whereas digital solutions such as e-government, e-commerce, e-education, e-health and e-environment are dependent on the use of ICT. Ultimately, even essential services such as water and electricity supply are more and more reliant on ICT[3] these days.

[1] https://www.internetworldstats.com/europa2.htm#kv

[2] The Digital Visualizer of Household Survey Data (DHS) is available at: www.undp.org/kosovo/digital

[3]: A Comprehensive National Framework on Critical Information Infrastructure Protection, 2007, is available at www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

The entirety of these actions strengthens the value of the public engaging with technology and the internet, but at the same time, they remain negatively correlated with the public's exposure to types of threats that would be impossible in an analogue reality. Therefore, opportunities arising from Kosovar's interaction with technology and the internet align with how well we acknowledge and tackle the challenges and vulnerabilities in the cybersecurity domain. Ultimately, this positions cyber security as a precondition for an accelerated digital transformation in Kosovo, one that is also in line with the Kosovo Digital Agenda 2030. This national strategy is an important part of realizing Digital Agenda goals.

2.1. Purpose

This strategic document aims to define objectives for the advancement of the general and specific capacities of the institutions of the Republic of Kosovo in the area of cyber security for the coming years. Furthermore, this document presents the vision of the Government of Kosovo on cyber security and defines the relevant action plan.

2.2. Vision

"The Republic of Kosovo will create a safe and resilient online environment for all citizens, businesses and the Government, working to predict and reduce vulnerabilities, and develop skills and capabilities to address cyber security issues while preventing and minimizing damages."

3. METHODOLOGY

The National Cyber Security Strategy's design is designed based on an assessment and analysis of Kosovo's institutions, law enforcement agencies, the needs of the private sector and local and international organizations, and global trends, as well as the European Union practices and policies. In this context, the Strategy is in full compliance with the ENISA guidelines and the EU member states' practices on strategies.

The methodology used during the work for the design of the National Cyber Security Strategy is presented in the following scheme:

Figure 1 - Methodology used during the work for designing the Strategy

1. **Establishing a working group, researching literature and public documents** - The Secretary General of the Ministry of Internal Affairs issued Decision No.973/2021 on 30.09.2021, establishing a working group for drafting the Cyber Security Strategy and the Action Plan. Representatives from public institutions, international experts, professional associations, the private sector, civil society and international partner organizations participated in the composition of the working group. The working group was tasked to draft the Cyber Security Strategy and the Action Plan at the national level.

2. **Organizing meetings and workshops with experts, representatives of institutions and stakeholders** - Meetings and several workshops were held with representatives of public institutions, local and international experts, representatives of international partner organizations and civil society for drafting the Cyber Security National Strategy. The first workshop was held on 20 and 22 December 2021, wherein it was reported on how to implement the first Cyber Security Strategy and the Action Plan 2016-2019. At the same time, the way how to organize the work for drafting the new Strategy was determined. The

second workshop was held on 17-18 March 2022, wherein the strategic and specific objectives for the new Strategy were discussed. The third workshop was held on 23.12.2022, wherein the Action Plan activities were discussed.

3. **Analyses and discussions -** The theoretical and empirical literature in the area of cyber security was analyzed and primary and secondary sources were used as basic materials, such as analyses and risk assessments by state institutions, the implementation of the first cyber security strategy, various publications of local and international organizations, expert opinions and evaluations, ENISA instructions and other relevant documents.

4. **Public and inter-ministerial consultations –** From 13.03.2023 to 03.04.2023, the strategy document was placed in public consultations. During this period, comments were received from local and international institutions.

5. **Finalization of the document of strategy –** After analyzing the comments, the strategy and action plan document was finalized.

4. GUIDING PRINCIPLES

The following are the guiding principles for the Government, businesses and the community.

4.1. Guiding principles for Government

While this document largely sets the parameters for a functional action plan and future steps towards a secure cyberspace, institutions must abide by the following principles to maximize the impact of a unified strategy:

1. Ensure that the frameworks and methods for identifying critical information infrastructure are in place and provide guidance to ensure that critical information infrastructure entities are identified and have the tools to reduce cyber risk.

2. Establish a clear cooperation framework with other countries to prevent, detect, alert and handle cyber incidents.

3. Promote international cooperation on cybersecurity and collaboration on combating cybercrime and developing cyber diplomacy.

4. Work to protect critical infrastructure, essential services and the community. As such, strives to protect the following:

- Protects government data, systems and networks.
- Creates mechanisms, guidelines and fora to support businesses to meet cyber security standards.
- Promotes an ecosystem of cybersecurity startups and attracts investment.
- Develops and maintains cybersecurity capacity building such as trainings for officials and a specific cybersecurity education curriculum for schools and universities.

5. Ensure that Kosovo continues its national approach to developing a legal framework on cyber security to make cyberspace a safer domain and help combat cybercrime.

6. Institutions, through their policies and administrative proceedings, assure that all approaches towards cybersecurity remain people-centered and intentionally inclusive for the whole of society.

7. Ensure that Kosovo will develop its capabilities for cyber security in harmony with the voluntary norms of GGE.

4.2. Guiding principles for the private sector

The following are some guiding principles which should be adopted by the private sector in order to have a prosperous nationwide approach to cyber security:

1. Private sector entities must enhance baseline security for all critical national infrastructure.

2. Private companies that own critical information infrastructure, should perform periodic risk assessments in order to identify vulnerabilities and mutual dependencies between infrastructures.

They should also establish security programs based on continuous improvement mechanisms to ensure that mitigation measures are efficiently and effectively implemented.

This will help ensure comprehensive securing of digital value chain.

3. Private sector entities must exercise due diligence in protecting their network and information systems and be the first responders in the case of cyber incidents.

4. Businesses and other agencies should invest in building a skilled cyber security workforce.

5. Cooperation between the private sector and the Government of Kosovo should be based on principles such as mutual trust, transparency, cyber threat and incident information sharing and sharing of expertise.

4.3. Guiding principles for the community

Finally, a safe cyber space cannot exist without the understanding and cooperation of the community. As such, the following principles should exist in the acumen of the community itself and should be observed in order to create a safe online space:

1. Each person has a responsibility to ensure that his or her computer, mobile phone or any ICT infrastructure at his or her disposal to be updated and to have malware protection.

2. Individuals have the responsibility to make informed purchasing decisions and to seek more information when not sure.

3. Individuals should report cyber-crimes in the same manner as they would treat any other crimes set within the legal framework of Kosovo Government.

5. CHALLENGES, RISKS, AND THREATS TO CYBERSPACE SECURITY IN KOSOVO

A clear understanding of the problem related to the provision of cyberspace in the Republic of Kosovo by all parties is essential to enable effective cooperation and coordination between the parties mandated and responsible in this area.

The protection of critical information infrastructure is essential for the Government of the Republic of Kosovo, especially since successful cyberattacks against this infrastructure would have a significant impact on the country. Such impacts can include destabilizing the economy and damaging the reputation of businesses and individuals. Therefore, it is of vital importance that the Republic of Kosovo pays attention to the protection of critical information infrastructure, which is essential for guaranteeing the provision of essential services.

The protection of critical information infrastructure requires the cooperation of all relevant actors, including public and private institutions that own or operate critical information infrastructure, which supports the proper functioning of society. In this regard, the activities should be addressed to all relevant actors to identify and understand the weaknesses and cyber security levels of the critical information infrastructure in general. Activities and actions will focus on relevant parties to establish measures that will address current and future cyber threats and risks to critical information infrastructure and drive improvements where needed.

As adversaries' cyber capabilities grow, they will pose increasing threats to security, including critical infrastructure, public health and safety, economic progress, and stability.[4]

Cyberspace can be considered a volatile terrain. Criminal activities are constantly creating a conflicting context, while state actors must combat criminal activities threatening governmental or economic sovereignty. Accordingly, a wide range of attackers, motives and techniques have evolved, which prove to be increasingly threatening to Kosovo.

Moreover, it should be noted that cyberspace is not only a virtual space but also part of socially important physical components and systems. Hostile actions in cyberspace can easily endanger the operation of critical infrastructures and essential services, becoming a threat of national proportions and to life. Finally, critical national infrastructure facilities, whether power plants, air transport facilities or other forms of public transport, are increasingly being targeted. Cyberattacks can disrupt power supplies to hospitals, homes, schools and factories.

Given that societies rely so heavily on efficient electricity supply, outages for extended periods of time would also have serious implications for other vital services.

https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

5.1. Threats

Cyber threats are already challenging public trust in global institutions, governance and even norms.

Cyber threats come from the opportunities and intentions of criminals to launch a cyberattack on ICT systems.

Cyberattacks can be motivated by:

- **Revenge:** Committed by staff within the organization or former (dismissed) employees;
- **Curiosity:** The so-called "script-kiddies" (young people who use ready-made scripts for attacks);
- **Monetary gain:** Committed by individuals or criminal groups;
- **Espionage:** Cyberattacks involving unnoticed intrusion of a third party to ICT Systems by reading, changing, deleting or even adding information. Such intrusions can also be used to misuse the communication and information systems attacked and to attack other systems;
- **National Security Breach:** Performed by actors sponsored by other states;
- **Cyber terrorism:** It involves highly targeted efforts with terrorist intent, which is an evolving threat and has the potential to cause serious damage. While terrorism is often associated with the loss of lives, we cannot overlook the significant consequences such as intimidation or coercion that can be brought about by cyber terrorism.

Extremist and radical groups are increasingly using cyberspace for organisation and media propaganda to promote their activities, recruit new members, and organize terrorist actions, which pose threats to the state security of the Republic of Kosovo.

Critical information infrastructure is continuously the target of cyberattacks. These attacks specifically aim at particular targets chosen by terrorists or hackers looking for sensitive information or to destroy this critical infrastructure.

5.2. Risks

- Lack of cyber security legislation defining minimum security measures for operators of essential services and digital service providers;
- Lack of risk assessments;
- Lack of a list of entities of sectors identified as national critical infrastructure, based on the Law on Critical Infrastructure.
- Lack of professional and technical capacities to prevent cyberattacks.
- Lack of citizens' awareness of the risks in cyberspace

- Lack of dedicated budget in state institutions and the private sector for cyber security

5.3. Addressing cybercrime

Cybercrime remains one of the challenges for the institutions of the Republic of Kosovo. The Republic of Kosovo has taken concrete steps in creating the legal infrastructure for preventing and combating all forms of cybercrime, but many challenges still remain, especially in the technical terms of successfully dealing with this form of crime.

Close cooperation between law enforcement agencies around the world is imperative in order to combat the rapid cybercrime growth.

The significant increase in the number of Internet users in recent years in the Republic of Kosovo induced an increased risk of crime and cyberattacks. Some criminal activities that have occurred are enough to highlight the weakness of computer networks considered to be in the development stage. According to available data, the main target of cyberattacks in the Republic of Kosovo has been the state computer network system, user accounts, banking system, websites and the private sector.

The capacities of law enforcement agencies in combating cybercrime, as well as in relation to protection against espionage and sabotage, should be further strengthened. Likewise, it is necessary to advance the institutional law enforcement mechanisms to combat cybercrimes and strengthen international cooperation in the exchange of information. In addition, there is a need to provide professional development and training for the officer of law enforcement institutions in order to enhance their capacities in prosecuting and detecting cybercrime.

Cybercrime requires a specialized response from institutions. Law enforcement agencies must be able to take coordinated action and investigate crimes against theft and misuse of data and computer systems, computer-committed crimes, and secure electronic evidence related to criminal offences.

5.4. Balancing security and privacy

Public and private authorities guarantee respect for fundamental rights and freedoms in accordance with the Constitution of the Republic of Kosovo. Fundamental rights must be guaranteed even within cyberspace. Increased cyber security may improve the protection of users' privacy and property in cyberspace.

The Government of Kosovo will continue to take the necessary measures to protect and guarantee cyber security. Such measures will respect privacy, fundamental rights and freedoms, free access to information and other democratic principles.

6. THE WAY FORWARD

All countries aim for an informed and functional National Cyber Security Strategy. Developing such a strategy and especially its successful implementation is not an easy task. Setting strategic priories is therefore crucial for the Republic of Kosovo.

The Government of Kosovo aims to outline its vision for a safe cyberspace for citizens, businesses and public institutions through 6 strategic objectives.

7. STRATEGY OBJECTIVES

Serving the overall vision, while taking into account the above listed considerations, the Strategy will work to achieve the following six strategic objectives and goals, within the 2023-2027 timeframe:

Strategic Objective 1: Create legal and institutional cyber security capacities at the national level.

Strategic Objective 2: Promote cyber security awareness and a cyber-security culture in Kosovo.

Strategic Objective 3: Support the development of the private sector in cyber security, Public-Private Partnership (PPP) and cross-sectoral information sharing.

Strategic Objective 4: Build sustainable and beneficial national and international cooperation in cyber security.

Strategic Objective 5: Develop lasting cyber security capacities for the government and the private sector.

Strategic Objective 6: Advance the investigative and military cyber security capabilities.

The scope of each objective is described below.

7.1. Strategic Objective 1: Create legal and institutional cyber security capacities at the national level

Supporting the continuity of essential services across Kosovo in the face of disruptive or targeted attacks remains a fundamental obligation of the Government. Disruption of critical societal services and functions like electricity, water, communication systems, command and control, air transport can have a devastating impact that can threaten national security.

In general, there is always more to be done in perfecting the overall security posture of critical infrastructure, some state and non-state actors are so sophisticated that an attack may be beyond the capability of a single network owner to handle alone, irrespective of its size, expertise, and best efforts. Therefore, this document outlines responses to Kosovo's evolving threat

environment with the aim to build thorough baselines, niche capabilities and partnerships that in sum will benefit all relevant stakeholders regardless whether from the public or private sector.

As such the document lays out the measures, roles and responsibilities of relevant stakeholders, in ensuring the security and resilience of Kosovo's critical national infrastructure and the potential of forging policies to forecast future threats and effectively take action in future emergencies.

7.1.1. Regulatory framework

The Government of Kosovo will introduce an improved regulatory framework to identify and protect CII entities from all threats, including dynamic and potentially catastrophic cascading threats enabled by cyberattacks. The framework will include specifications on security obligations for national critical infrastructure entities with sector-specific requirements. This is consistent with cyber, physical, personnel and supply chain protections across all sectors, while recognizing that there are sector specific differences. These differences can be found in human and financial resources, specific technologies, types of threats, existing standards and maturity of different entities.

7.1.2. Guidelines

Specific guidelines will be developed to identify vulnerabilities and dependencies between infrastructures to ensure a proper security posture of digital supply chains. The guidelines will include a range of activities that aim to improve the collective understanding of risk within and across relevant sectors. The Government will propose minimal technical standards including certifications for secure technology and security technology.

In addition, Kosovo Government will issue informed, security guidelines, for the procurement of IT in general. For all NCIs, there will be enhanced sample auditing measures involving the critical supply chain.

7.1.3. Periodic audits

Furthermore, there will be periodic audits that will be implemented, being among the key measures that enable the assessment of the effectiveness of the security management systems currently implemented, including the adequacy of the introduced safeguards. Audit methodologies should take into account the applicable standards, good practices and specifics of the respective sectors. Fully utilizing this approach, ensures the achievement of comparability between audit outcomes.

A successful audit process should contain the following elements:

1. Device mapping, criticality mapping, accessibility mapping;
2. Vulnerability mapping, including:
    i. Penetration testing;
    ii. Defect rate analysis;
    iii. Security culture and architecture analysis of NCIs and selected components at vendors;

iv. Security capacities of NCIs and contractors, and contracting options.

Periodic testing, which provides a realistic assessment of the system's resilience to threats, is another security measure. Outcomes of these tests create the basis for verification of the safeguards deployed. In order to utilize the public capacity in the area of cyber security, *bug-bounty* testing shall be disseminated.as well. To ensure the operation of the critical infrastructure in the ICT sector, it is vital to conduct regular assessment of risks to the operation of the critical infrastructure of the ICT sector, planning the appropriate protection measures and updating the risk assessment.

7.1.4. Approaches to protect critical infrastructure

Updates must be performed by trusted or security-cleared personnel from vendor companies. All NCIs must have their own CSIRT structure or at least an information security officer. National sectoral CSIRTs may be established for specific sectors of national critical infrastructure, which will be responsible for the entities that are part of that sector at the national level.

Critical infrastructure is increasingly interconnected and interdependent, which without proper safeguards creates vulnerabilities and can deliberately or inadvertently cause disruption that could result in cascading consequences across Kosovo's economy and national security. Recent incidents in Kosovo, but also across the world, including impacts from COVID-19, demonstrate that those threats could be significant to the functioning of critical infrastructure entities.

Cyberattacks can have major consequences for vital societal functions and critical IT systems, and can be considered similar to a conventional armed attack, can therefore in certain cases can also be considered as an armed attack. An analysis of CII ought to be carried out to support ongoing mapping of Kosovo's mapping of critical infrastructure. The purpose is to equip society to continue vital societal functions in a better way if these are affected by major cybersecurity incidents. Effectively securing these systems, and data within them, is a matter of national security and sovereignty. The Government of Kosovo will consolidate its information technology infrastructure to further enhance its security.

The strategy launches a series of strategic actions to strengthen the security of vital societal functions and ensure that government agencies and businesses have an adequate level of security. Some of the key measures include:

1. All Government agencies must comply with international standards defining best practices in information security management.
2. Security requirements for the management of government ICT systems critical to society will be tightened to ensure that security in and around ICT systems has the right managerial focus.
3. Embedding and prioritizing cyber and information security at all levels of management will be ensured by strengthening the knowledge, awareness and behavior of top managers

in government through increased requirements and expectations as well as new skills initiatives.

Common technical solutions, such as DNS, are being established to strengthen security among government authorities. Deploying DNS will strengthen the technical security posture of the NCI operators and improving the capacity of their technical staff to identify and implement effective and customized solutions.

Therefore, the Government of Kosovo seeks to ensure that appropriate steps are taken to ascertain that all national CII are identified and properly protected from a variety of threats. It is also noted that a more secured CII will help to achieve the continued provision of essential services and support national security, economic prosperity and social well-being of Kosovo.

Attacks can also be directed against our fundamental values and the democratic functions of society, for example through disinformation and influence campaigns. Disinformation can be used to intentionally disseminate untrue or misleading information in order to influence people's attitudes, standpoints and actions in a certain direction. Influence campaigns are centrally controlled, and involve and use a broad spectrum of methods, both open and covert, a subset of which might be data intrusion and other cyberattacks. It can also include political, diplomatic, economic, and military instruments of power. The dissemination of incorrect or misleading information risks undermining confidence in our public institutions and challenges the security. Critical handling of information sources and access to a diversity of independent media and news agencies strengthen awareness and counteract the effects of disinformation and influence campaigns.

7.1.5. National model for systematic cyber security efforts

As outlined above, information society, electronic government, and digital economy are going through a rapid pace of development. Simultaneously, cyberspace is being met with new threats. More than ever before, a structured national cybersecurity system should be improved and developed so that it is able to face and cope with new challenges being presented. The governing structure which should lead the work in the area of cyber security in Kosovo is presented below. The development of cyber security nationwide is the key objective of the Strategy, requiring first of all further development of the structures dealing with cyber security at the strategic and operational levels.

To make these developments possible, the Government of Kosovo will introduce a new legislation on cyber security, which will define the revised competencies of the relevant institutions with respect to cyber security. Based on the respective legislation, ***Cyber Security Agency (CSA***) will be established as an executive agency which will regulate the responsibilities of two main categories of entities: ***Operators of Essential Services*** (OES) and ***Digital Service Providers*** (DSP). The categories of OES are public or private entities that own NCI based on Law on Critical Infrastructure. With the approval of this cyber security legislation, the proposed governance structure of cyber security in Kosovo will look like the following:

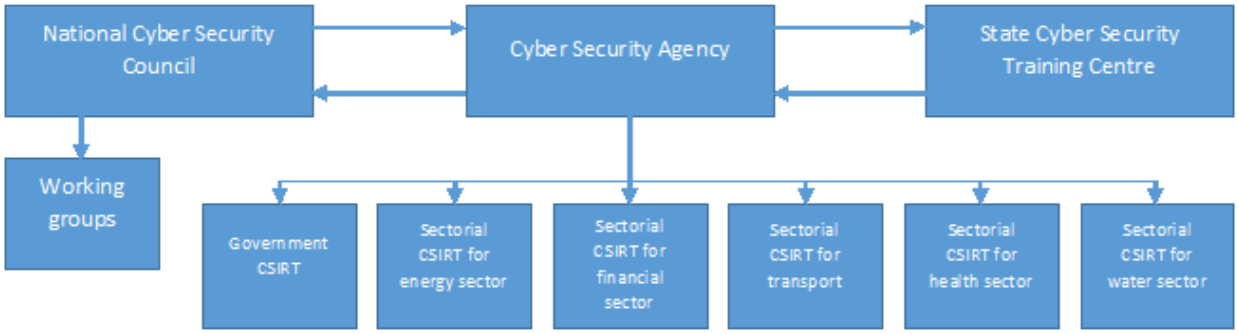

Figure 1. Governing structure of cyber security in Kosovo

7.1.6. **Institutional harmonization**

Currently, the activities and institutional responsibilities in the area of cyber security are fragmented and distributed between different public and private sector entities, resulting in limited efficiency in this area. To improve this situation, it is necessary to have consolidation and harmonization of the duties and responsibilities of the various institutions responsible for cyber security. Institutions, or better said, stakeholders involved in cyber security, should work closely with each other to identify their roles and responsibilities, as well as the resources available to them, and provide open and transparent input to the National Council for Cyber Security (NCCS) and the Cyber Security Agency (CSA).

It is necessary to set up systemic solutions to exchange information between stakeholders and share knowledge about vulnerable or ineffective technology, threats and cyber security incidents. To ensure that the entire ecosystem will function effectively, the relationship between all stakeholders in the national cyber security system, including authorities in charge of national security, counter-terrorism, internal security and public order, public prosecution and the judiciary must also be clarified. The overlapping of legal responsibilities should be reduced, while contradictions should be identified and avoided.

- National Cyber Security Coordinator (NCSC*)* will be the person heading the NCCS.

NCSC coordinates, in accordance with the applicable legislation, activities with the relevant technical or executive decision-makers of all stakeholders. Such decision-makers will, in turn, have to communicate at the working level with suppliers, partners, and their networks, or even establish forms of cooperation wherein they will discuss, evolve and implement strategic initiatives.

Responsibilities and coordination in the national cyber security system will be more precisely defined by by-laws. This will include the obligations and powers of the system mechanisms and entities, as well as the ways in which the NCSC can work with the system stakeholders. NCSC and NCCS must take care to avoid overlapping, build and distribute resources, implement inter-

governmental cooperation and public-private partnership, and rigorously identify and eliminate dysfunctional activities and personnel.

- The Critical Infrastructure Cybersecurity Working Group (CICWG) will be a multistakeholder advisory group, under the auspices of the NCCS**.** *The goal of the Working Group is to provide* overall support on increasing cybersecurity resilience of NCI's cyber security. The group will consist of representatives from relevant Government agencies and ministries, the private sector and academia. This will ensure that all relevant stakeholders contribute to drafting policies, create opportunities for dialogue between the public and private sectors, and help obtain support from stakeholders for the implementation of new policies in the area of cyber security.
The Critical Infrastructure Cybersecurity Working Group aims to:

i. Build institutional capacity to advance cyber security resilience of NCI,
ii. Establish a national cyber security information-sharing platform, and
iii. Drive forward the development of cyber security institutions in the Republic of Kosovo.

7.1.7. **Risk management system at the national level**

The **NIST[5] Cyber Security Framework** incorporates risk management as one of its core principles and expects that adopters of the framework will practice risk management and undertake related activities. However, each country decides how to practice the risk management provided in this framework. In order to advance cyber and national security, CSA should adopt a coherent national cyber risk assessment system. This risk assessment system should take into consideration the specifics of the NCI's sectors and operators, as well as digital service providers. CSA will carry out technical and tactical monitoring of the capacities of various actors to deal with relevant cyber threats.

This also includes coordinating knowledge of vulnerabilities and threats within the national cyber risk assessment system. Risk assessments can also be supported by qualified academic staff.

In addition, the Government of Kosovo also aims to establish the ***National Flash Reaction Team*** **(NFRT)**[6], as a body that will offer concrete technical assistance in the necessary actions to tackle threats or vulnerabilities.

NFRT will have a regular monitoring role, including periodic checks for vulnerabilities and patches by maintaining a frequent contact with the security departments of equipment and system manufacturers. NFRT shall produce an *implementation guideline* for all patches and workarounds, or when deemed necessary, video instructions within 24 hours of the release of a new patch or a workaround. A highly secure communication pattern must be set up to all affected parties. The NFRT should communicate frequently with manufacturers and operators and build trust and cooperation. The NFRT can also be offered to friendly neighboring countries as a diplomatic tool

[5] https://www.nist.gov/

to educate and assist and as a CSBM. In turn, countries are likely to appreciate the informed help and be more open for other forms of cooperation, thus increasing the cooperation network.

NFRT will be structured within the CSA and will help prepare the national threat and risk assessment based on an established risk assessment methodology. CSA will monitor and carry out re-assessments on a regular basis, the results of which must also be published in the annual report.

Once maturity is reached in its operation, CSA will work on the development of a cyber range[7] to test and implement new technologies and use them in various technology initiatives. Findings should be kept updated and shared with IT vendors on a basis of mutual trust.

When not in use by the CSA and Government institutions, the cyber range can be rented out to Kosovo's cyber security startups to promote their development, train their red teams playing the role of an enemy or competitor, and do internal testing of the maturity of their products.

One of the mechanisms that should be implemented is the establishment of a reward system for reporting vulnerabilities. Confidence building remains the main prerequisite for reporting and information sharing.

The six specific objectives which will help to implement the general strategic objective 1 are as follows:

- ***Specific Objective 1:*** Develop the legal framework on cyber security and protection of NCI in accordance with the EU acquis. This framework should align with directives and regulations stemming from the European Union.
- ***Specific Objective 2:*** Establish a NCI catalogue; assess the current cyber security maturity and draw up a multi-year plan to achieve the necessary protection level.
- ***Specific Objective 3:*** Build central national cyber security authorities mandated to enforce laws, develop and oversee the implementation of the national strategy and harmonize efforts at the highest level.
- ***Specific Objective 4:*** Strengthen the national CERT and other cyber incident response capacities by building a larger effective workforce, and extending its responsibilities and capabilities related to the NCI cyber security. This includes an audit function for auditing and publishing the effectiveness of cyber security technologies and an information-sharing function across the Government entities.
- ***Specific Objective 5:*** Issue effective technical standards for different security levels, publish guidelines[8] and extend a support function for the implementation and maintenance of standards.

[7] https://www.cyberwiser.eu/content/what-cyber-range
[8] https://www.ncsc.gov.uk/section/advice-guidance/all-topics

- **Specific objective 6:** Develop a national strategic approach for the procurement and operation of the least vulnerable information technologies in the government and critical private sectors. This includes a legal framework for regular backup[9] and rapid patching.

7.2. Strategic Objective 2: Promote cyber security awareness and a cyber-security culture in Kosovo

A better understating of the threats cyberspace faces, is crucial step to being able to combat them. While the Government of Kosovo does recognize its role in creating a more secure environment for all its citizens, the Government jointly with the private sector and the community have an important joint role to implement this Strategy. Therefore, the successful implementation of this Strategy relies on individual and collaborative efforts and actions by all relevant stakeholders. The Government of Kosovo will strive to build an effective and inclusive public-private partnership system based on mutual trust and shared responsibility for our national cyberspace security. Collective steps must be taken to protect Kosovo from possible attacks, hostile propaganda or any other form of disruption.

In support of this objective, the Government will create a research and development system for projects that include and go beyond the area of traditional cyber security to understand existing and potential threats, including cyberstalking, hate speech and disinformation. Competency and knowledge of threats, vulnerabilities and effective measures are a prerequisite for protecting CII. With the development of IoT, smart cities, *Industry 4.0, Cloud Computing* and *Big Data*, there is a need to increase the cyber security research and development activities.

In terms of skills and areas of interest, research aimed at building national encryption capabilities and developing a national encryption algorithm for national needs could prove useful. Otherwise, it should be proceeded with well-known encryption algorithms such as *RSA*[10] or similar.

In addition, basic cyber security courses will be developed. Such courses will include a curriculum that teaches the basics of hacking, at the university level, but more importantly, a version of it will be developed for high school students, making sure to be inclusive, attractive course and to involve young girls who would benefit greatly from such knowledge and help close any gender gap.

There is a clear cyber security skills gap reported in Kosovo's public administration in terms of the shortage of qualified human resources to work in this field. And the gender gap in this area is even more obvious.

[9] Published vulnerabilities are quickly exploited as attacking tools used against targets by most hackers. If the patch time is less than or equal to the time needed to exploit the vulnerability, such hackers are denied the opportunity to attack. The only remaining possibility of attack is by hackers using zero-day vulnerabilities, which are much rarer and mostly attack only high-value targets. Patching software therefore quickly reduces many risks.

[10] RSA: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Cyber security specialists must cover the labor market needs and national security requirements. Bringing more women and girls into cyber security would boost the industry and meet the dire need across sectors and stakeholders for top talents.

A long-term inclusive plan should be drawn up to build national capacities in this area, including awareness-raising measures among the general public. Cyber hygiene [11], digital skills, awareness of modern cyber threats and dealing with them should become an integral part of the education of every citizen of Kosovo.

Strategic Objective 2 will be implemented with the help of the following four specific objectives:

- ***Specific Objective 1:*** Develop and implement awareness-raising campaigns that will cover different sectors within the Government and other public institutions, NCI's, the private sector and civil society;
- **Specific Objective 2**: Create civil and academic outreach campaigns, conferences and programs, involving all parts of the society in fostering an ongoing dialogue about cyber security;
- **Specific Objective 3:** Promote university research and development, teaching and training in cyber security and data protection;
- **Specific Objective 4:** Establish a STEM education program in schools, incorporating cyber security components to inspire more girls in choosing to work with cybersecurity as a career. This should be considered a high priority as it easily doubles the existing workforce.

7.3. Support the development of the private sector in cyber security, Public-Private Partnership (PPP) and cross-sectoral information sharing.

Ensuring the security and resilience of Kosovo's digital domain and infrastructure, is a shared responsibility among multiple stakeholders. This is especially true given that neither the Government nor the private sector alone has the knowledge, authority or resources to carry this responsibility exclusively.

Public-private partnerships are the foundation for an effective implementation of the security strategy, and timely, trusted information sharing among stakeholders is essential for the security of Kosovo.[12]

Setting up a Public- Private Partnership (PPP) framework will enable knowledge exchange, sharing of best practices and common level of understanding among all stakeholders. According to ENISA[13] the main motivation from the public and private sector to join in PPPs is to raise the level of cyber security. Increased collaboration will lead to: better situational awareness, better

[11] Cyber hygiene is a set of practices that organizations and individuals perform regularly to maintain the health and safety of users, devices, networks and data. The goal of cyber hygiene is to keep sensitive data safe and protect it from theft or attacks.
[12] European Union Network and Information Security Agency (ENISA): Public-Private Partnership (PPP) Cooperation Models, November 2017.
[13] Ibid.

decision-making, an increase in trust, better access to resources and a better understanding of CII protection and cyber security in general.[14]

PPP arrangements enhance communication, planning, risk assessment, program implementation, and operational activities, including incident response and recovery. Such partnerships will help to implement security and resilience activities across Kosovo and will be embedded in the national cyber security system.

The Government of Kosovo must develop a system to promote the establishment of cyber security *start-ups* in Kosovo. There is a visible talent for innovation in Kosovo, and startups provide a better incentive structure for young talents to bind them to the cause of cyber security nationally. Cyber security startups can be funded with international investment, if some attractive conditions like low taxes and government contracts for functioning products can be offered. They can help create a large specialized workforce to support the overall cyber security operations and bring economic benefits to Kosovo. Creating an effective core of knowledge and training motivated by entrepreneurship and informed by industry is essential for establishing such a *start-up* culture, which can be developed in applied universities or the military, with efforts already underway to create a cyber-security training centre.

Strategic Objective 3 will be implemented with the help of the following two specific objectives:

- ***Specific Objective 1:*** Create Public-Private Partnership working groups and incentivize the establishment of special working groups within the private sector to share information on cybersecurity threats and products

- **Specific objective 2:** Develop incentives and a nucleus for cybersecurity startups in Kosovo, as well as invite foreign strategic and financial investments through special and attractive investment mechanisms. This should be considered a high priority as it can solve many issues sustainably while being funded externally and generating economic benefits for Kosovo in the long run.

7.4. Strategic Objective 4: Build a sustainable and beneficial national and international cooperation in cyber security

A. International cooperation at the strategic and political level

In order to promote a secure and reliable international cyberspace, and in support of national interests, the Government of Kosovo will engage internationally in:

[14] European Union Network and Information Security Agency (ENISA): Public-Private Partnership (PPP) Cooperation Models, page *13*, November 2017.

a. Increasing Kosovo's presence in international and regional cyber security organizations and forums.
b. Promoting international cooperation in the legislative, judicial and police sectors in combating cybercrime and cyber espionage;
c. Improving the diplomatic communication protocol and procedures in order for Kosovo to become a trusted and credible international partner in combating cyber threats and in the unified stance to protect human rights in cyberspace.
d. Fostering cooperation with NATO in Cyber Defense, particularly with respect to responding to cyber incidents and exchanging technical information on threats and vulnerabilities;
e. Promoting the international policy in cyberspace with a view to cooperation and alignment of national legislation with the European Union.

B. **International cooperation at the technical and operational level**

International cooperation with the EU, NATO and other friendly countries should be strengthened. Such a situation should be aimed at, where carrying out cyberattacks against Kosovo will be difficult and have consequences for the attackers. Kosovo must actively contribute to ensuring an open, secure and reliable Internet space, as well as to the protection of critical ICT infrastructure and CII.

In addition, Kosovo should also participate in international technical dialogue and develop its international network by learning from the experience of international institutions and partners that work successfully in cyber security.

Kosovo institutions will make efforts to identify and join the technical exercises and international standardized training. Kosovo will strengthen international cooperation in cyber security by supporting international initiatives that fulfil Kosovo's national interests and expand Kosovo's dialogue with the EU, NATO and OSCE. In order to strengthen cyber security defense and diplomacy, Kosovo will take the following actions:

a. Establishing cooperation with the Internet Corporation for Assigned Names and Numbers (ICANN) to develop public policies on the Internet;
b. Exploring the possibilities for Kosovo's membership in the EU Strategy to implement *DNS* and to diversify the *DNS* name recognition, as well as support the *DNS4EU* initiative to avoid extreme scenarios of cyberattacks on the global root of the *DNS* system;
c. Exploring the possibilities for the adoption and implementation of the EU IPv6 regulation, not only for economic reasons but also for law enforcement purposes;
d. Strengthening cooperation with the European Union Network and Information Security Agency (ENISA), specifically, but not limited to, incident response, threat detection and workforce development;
e. Establishing cooperation with the International Telecommunication Union (ITU) in the standardization of cyber security and electronic communications;

f. Increasing bilateral and multilateral cooperation with the national CERTs of other countries.

Strategic Objective 4 will be implemented with the help of the following three specific objectives:

- **Specific Objective 1:** Foster national cooperation across all sectors and open Kosovo as a competent actor for international cooperation regionally and globally
- **Specific Objective 2:** Participate in diplomatic efforts around cyber norms
- **Specific Objective 3:** Join cybersecurity and cybercrime conventions and other relevant international agreements
- **Specific Objective 4:** Offer Kosovo as a ground for military cyber exercises and participate in cyber exercises

7.5. Strategic Objective 5: Develop long lasting cyber security capacities for Government and the private sector

Developing sustainable capacities represents probably the biggest challenge in cyber security. A large number of countries and many companies are failing in this regard, and this has a major impact on the overall strategic standing and security posture. The development of human resources and competent staff takes a long time, at least several years. In addition, the ICT workforce can be quite volatile in terms of switching employers, and this is particularly true in the case of ICT professionals in the public service, and the transition of competent workers to the private sector. Even within the private sector, there is a lot of competition and movement of workers.

Capacity building and retaining competent staff is a key priority for Kosovo. The dynamic nature of cyber security challenges requires the continuous development of the necessary capacities and skills. The Government of Kosovo will therefore promote:

g. Developing a capacity-building plan to address Kosovo's specific requirements for the skills needed to meet the ever-increasing challenges of addressing cyber security threats, and
h. Developing recruitment and retention strategies aimed at ensuring the development and maintenance of a sufficient level of expertise.

Strategic Objective 5 will be implemented with the help of the following three specific objectives:

- ***Specific Objective 1:*** Open up key government functions to private sector support or partial outsourcing to fill critical knowhow gaps. This is a measure that may be seen as unusual, but it is important to fill such gaps.
- ***Specific Objective* 2**: Develop a national training and education program on cyber security in the academic sector in cooperation with specialized entities of the private sector;
- **Specific Objective 3:** Reform the public salary and procurement mechanisms to open up Kosovo for costly experts inside government and for rapid procurement of critical technologies.

7.6. Strategic Objective 6: Advance investigative and military cyber security capabilities

The borderless nature of cybercrime, has contributed to the wide-spreading of criminal activities where computers and information systems are involved, either as a primary tool, or as a primary target. Cyber threats come from both non-state and state actors. They are often criminal in nature, motivated by profit, but can also be political and strategic. Therefore, cyber security is increasingly becoming a critical issue for national security. As such, cybercrime has an impact not only on the economy but also on the functioning of democracies, social freedoms and human values.

The blurring of the border between cybercrime and "traditional" crime, intensifies the criminal threat, as criminals use the internet both as a way to scale up their activities, and also as a source to find new methods and tools to commit a crime. Yet in the vast majority of cases, the chances of tracing the criminal are minimal, and the chances of prosecution are even smaller.

The Government of Kosovo has taken the necessary steps in establishing the legal infrastructure aimed at preventing and combating all forms of cybercrime. The "Cyber Crime Investigation Unit" within the Kosovo Police has the necessary technical capacities and training to investigate computer crimes.

However, many challenges remain especially technical challenges that prevent authorities from successfully dealing with this form of criminality. While initial steps have been taken, a more effective law enforcement response focusing on the detection, traceability and prosecution of cyber criminals remains to be established. It is essential to build trust among citizens that all types of crime are dealt with responsibly and effectively.

In recent years, a significant increase in Internet users has been observed in Kosovo, which has incurred an increased risk in terms of computer crimes and cyberattacks. Although there have been no cases of penetration and serious damage to systems with state data so far, various criminal activities have sufficed to highlight the weaknesses of computer networks in Kosovo. According to available data, the main targets of computer attacks in Kosovo so far are user accounts, banking systems and websites. The Government of Kosovo will improve the conditions for the police to perform their duties in accordance with technological developments and crime trends.

Many of the passive security mechanisms do not deter attackers. Such mechanisms simply increase the effort and time attackers have to spend to carry out the attack. Investigative capacities can also increase the risk to attackers. Therefore, the basic capability to investigate criminal or espionage incidents is very important.

Although investigations in some cases may not yield the desired results, not having investigative capacities cannot be seen as an option, as this would turn Kosovo into a target or proxy for attacks, generating many criminal and diplomatic problems for the country. Possessing good

investigative capabilities can even help Kosovo a lot to become an important international actor and build trust and relations with other countries.

The Government of Kosovo intends to develop functional and robust investigative capabilities. In order to strengthen investigative capabilities, the Government of Kosovo will, inter alia:

a. Improve legislation by addressing current challenges and trends in the area of cyber security;
b. Develop a methodology for collecting cyber statistics and annually publish statistical information on cyberattacks;
c. Ensure an increase in the level of knowledge of operation officers, employees of investigation authorities, prosecutors, and judges in the area of information technology and cyber security, and more specifically in the collection and securing digital evidence.
d. Facilitate the engagement of private sector experts in research in the area of computing and telecommunications, in the area of software and other necessary areas, which will allow them to respond quickly to cyber incidents and effectively investigate cybercrimes.

The activities planned for this strategic objective will be classified and will not be public.

8. RESPONSIBLE INSTITUTIONS AND LEGAL FRAMEWORK

8.1. Institutional mechanisms

The institutional mechanisms mean all the mechanisms having a role and importance in cyber security in Kosovo.

The institutional mechanisms for the design and implementation of state policies in the area of cyber security are, but not limited to, the following institutions:

Office of the Prime Minister
The Office of the Prime Minister is responsible for preparing the proposals for draft constitutional amendments, draft laws, draft by-laws, concept documents (impact assessment), ex-post evaluations of legislation, strategic documents and other proposals within the scope of the Government as a whole and Office of the Prime Minister, as well as monitoring and ensuring their implementation. The role of Prime Minister Office is to support implementation of strategic objectives;

Ministry of Internal Affairs
The Ministry of Internal Affairs is the institution responsible for drafting and monitoring policies and legislation in the area of cyber security in the Republic of Kosovo. Ministry of Internal Affairs also has a key role in coordinating the Strategy, monitoring the implementation of the Action Plan, and drafting periodic reports.

The Ministry of Internal Affairs is the institution responsible for the implementation of the Law on Critical Infrastructure and for identifying the NCI in the Republic of Kosovo.

Kosovo Police, as a law enforcement agency within the Ministry of Internal Affairs, has a key responsibility in combating all forms of cybercrime.

Agency for Information Society (AIS)
Agency for Information Society coordinates, leads and supervises the processes and mechanisms of electronic governance in relation to the ICT infrastructure, the expansion of Internet services in the institutions of the Republic of Kosovo, the accumulation, administration, dissemination and storage of data, establishing the State Electronic Data Center as well as the ensuring security and protection of the electronic and data communication infrastructure. As appropriate, AIS assists the relevant institutions in combating cybercrime and ensures the protection of personal data in electronic form, in accordance with the applicable legislation.

National Cyber Security Coordinator
The Minister of Internal Affairs, or a person duly authorized by him/her, who is responsible to coordinate, guide, monitor and report on the implementation of policies, activities and actions related to Cyber Security, will serve as a National Cyber Security Coordinator.
The State Cyber Security Council is headed by the National Cyber Security Coordinator.

Secretariat of strategies
The function of the Secretariat of strategies is to collect information and data from other institutions, analyze and assess the collected information, as well as draft analytical reports for the National Coordinator and the National Cyber Security Council. In addition, the Secretariat will distribute timely information to all relevant parties, thus supporting the cyber security action plan.

Department for Cyber Security and Systems Administration
The Department for Cyber Security and Systems Administration of the Ministry of Internal Affairs is responsible for the preparation of cyber security policies and the supervision of their implementation. It has a leading role in the preparation of the strategy.

Kosovo Judicial Council
It ensures that the courts in Kosovo are independent, professional and impartial, in order for the judicial system to be as efficient as possible in combating cybercrime.

Kosovo Prosecutorial Council
It ensures that the prosecutorial system in Kosovo is independent, impartial and professional in prosecuting, investigating and detecting criminal offences of cybercrime and representing before the courts the accusatory instruments on behalf of the state.

Prosecution Offices and Courts
They are the institutions responsible for the criminal prosecution of the perpetrators, their adequate punishment, for the confiscation of property and assets acquired through criminal activities.

Secretariat of Kosovo Security Council
The Secretariat, as an integral part of the Kosovo Security Council, prepares periodic reports and analyses for the Government of the Republic of Kosovo and the Kosovo Security Council related to political security issues, as well as assists in drafting security policies in Kosovo, including capacity building, policy and research instruments, providing administrative and operational support to the Kosovo Security Council.

Kosovo Intelligence Agency (KIA)

KIA identifies threats that endanger Kosovo's security. A threat to Kosovo's security is considered a threat to territorial integrity, the integrity of institutions, constitutional order, stability and economic development, as well as threats to global security to the detriment of Kosovo.

Ministry of Justice
The MoJ prepares and develops legislation in the area of justice, as well as coordinates and develops international legal cooperation in criminal matters.

Ministry of Defense (MoD)
The Ministry of Defense drafts the general state defense policies, while the Kosovo Security Force (KSF) implements such policies to protect the sovereignty and territorial integrity, citizens, property and interests of the Republic of Kosovo. MoD\KSF develops and strengthens cyber protection for MoD\KSF systems based on information technology and provides support to RKS institutions in case of crises in the country for the protection of data and critical infrastructure. Through the Cyber Security State Training Center, MoD\KSF will deliver training in the area of cyber security for all institutions of the Republic of Kosovo.

Ministry of Economy
It ensures the quality of services and technical standards in the area of telecommunications, creates work policy for the promotion of competition in the area of telecommunications, examines the needs and demands of consumers in the area of telecommunications, supports information technology and innovations, supports access to technology for all citizens of Kosovo and promotes the development of training systems in information technology.

Ministry of Finance, Labor and Transfers
MFLT ensures that the financial costs of Strategy activities are within the budget framework. Also, through Customs, the Financial Intelligence Unit and the Tax Administration will help strengthen cyber security and prevent and combat cybercrime.

Ministry of Education, Science, Technology and Innovation (MESTI)
MESTI plays an important role in the area of prevention and awareness raising through designing the curricula and organizing awareness-raising activities for the use of the Internet and other extra-curricular activities.

Ministry of Foreign Affairs and Diaspora (MFAD)
MFAD has a role in assisting in cyber diplomacy and international cooperation in the fight against organized crime.

Regulatory Authority of Electronic and Postal Communications (RAEPC)

RAEPC is a regulatory body, which implements and supervises the regulatory framework defined by the Law on Electronic Communications, and Law on Postal Services, as well as by the development policies in the area of electronic communications and postal services.

Kosovo Forensics Agency

It is the institution responsible for providing impartial, objective and professional forensic scientific expertise. The mission of the Kosovo Forensics Agency is to provide quality forensic services through the exercise of its activity in accordance with the applicable legislation, and local and international standards.

Information and Privacy Agency (IPA)

IPA ensures that controllers comply with their obligations regarding the protection of personal data and that data entities are informed of their rights and obligations in accordance with the Law on Protection of Personal Data. It also provides advice to the Assembly of the Republic of Kosovo, the Government, local government bodies and all public authorities in Kosovo regarding Personal Data Protection issues, as well as advises all private institutions regarding Personal Data Protection.

8.2. Legal framework

In the area of ICT, the Republic of Kosovo has in place a wide legal base, which includes but is not limited to:

- Constitution of the Republic of Kosovo[15];
- Law No. 06/L-014 on critical infrastructure[16];
- Law No. 08/L-173 on cyber security[17];
- Law No. 03L-050 on the Establishment of the Kosovo Security Council[18];
- Law No. 04/L-145 on Information Society Government Bodies[19];
- Law No. 04/L-094 on Information Society Services[20];
- Law No. 04/L-109 on Electronic Communications[21];
- Law No. 05/L-030 on Interception of Electronic Communications[22];
- Law No. 06/L-082 on Protection of Personal Data[23];
- Law No. 04/L-076 on Police[24];

[15] http://gzk.rks-gov.net/ActDetail.aspx?ActID=3702
[16] https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313
[17] https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933
[18] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2521
[19] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8669
[20] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2811
[21] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851
[22] https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968
[23] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2676
[24] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2806

- Law No. 03/L-142 on Public Peace and Order[25];
- Law No. 03/L063 on Kosovo Intelligence Agency[26];
- Law No. 04/L-149 on Execution of Criminal Sanctions[27];
- Law No. 4/L-065 on Copyright and Related Rights[28];
- Law No. 03/ L-183 on Implementation of International Sanctions[29];
- Law No. 04/L-213 on International Legal Assistance in Criminal Matters[30];
- Law No. 04/L-052 on International Agreements[31];
- Law No. 04/L-072 for State Border Control and Surveillance[32];
- Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Bank Financial Institutions[33];
- Law No. 04/L-064 on Kosovo Forensics Agency[34];
- Law No. 04/L-198 on Trade of Strategic Goods[35];
- Law No. 04/L-004 on Private Security Services[36];
- Law No. 06/L-123 on Kosovo Security Force[37];
- Law No. 06/L-122 on the Ministry of Defense - a *reference to be given*
- Code No. 03/L-109 Customs and Excise Code of Kosovo[38];
- Law No. 04/L-099 on Amending and Supplementing Customs and Excise Code in Kosovo, No. 03/l-109[39];
- Law No. 03/L-178 on Classification of Information and Security Clearances[40];
- Criminal Code of the Republic of Kosovo No. 04/L-082[41;;]
- Criminal Procedure Code No. 04/L-123[42;;]
- Law No. 03/L-122 on Foreign Service of the Republic of Kosovo[43];
- Juvenile Justice Code No. 03/L-193[44];
- Regulation No. 18/2011 on the Distribution and Transfer of Classified Information[45].

[25] http://gzk.rks-gov.net/ActDetail.aspx?ActID=2651
[26] https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2538
[27] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8867
[28] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2787
[29] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2674
[30] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8871
[31] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2789
[32] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2801
[33] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2816
[34] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2781
[35] https://gzk.rks-gov.net/ActDetail.aspx?ActID=8860
[36] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2741
[37] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2523
[38] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[39] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2600
[40] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2690
[41] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2834
[42] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2861
[43] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2615
[44] https://gzk.rks-gov.net/ActDetail.aspx?ActID=2698
[45] http://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=10554

- Law No. 06/L-014 on Critical Infrastructure[46]
- Law No. 08/L-022 on Electronic Identification and Trust Services in Electronic Transactions[47]

This Strategy is in accordance with international acts regulating the area of cyber security.

[46] https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313
[47] https://gzk.rks-gov.net/ActDetail.aspx?ActID=51618

9. IMPLEMENTATION, MONITORING AND REPORTING GUIDELINES

The following guidelines are designed to assist and guide all ministries to implement individual measures efficiently.

1. ***Security****:* The operation and further development of IT systems must be based on a comprehensive security philosophy including strategic, organizational and technical elements, such as security by design. A common approach must therefore be drawn up for all institutions.
2. ***A risk-based approach***: The strategy is based on a comprehensive risk-based approach aiming to identify and prioritize the most likely and most serious risks, and develop appropriate countermeasures to deal with them.
3. ***A multi-stakeholder approach*:** As part of the cooperative approach, all relevant stakeholders are to be involved in discussions and be given the opportunity to influence the processes and activities whenever possible. It is particularly important to ensure that measures taken in the public and private sectors are complementary.
4. ***Conformity with the EU*:** Priorities and developments at the European Union level have to be taken into account when implementing measures.

The National Cyber Security Council will do systematic monitoring and coordination of the implementation of the National Cyber Security Strategy taking into account all existing and future challenges in the field of cyber security.

Monitoring of the implementation of the objectives and activities of the action plan will be based on these key elements:

- The periodic progress report on the achievement of strategy objectives and implementation of the action plan will be drafted.
- The annual progress report will provide information on the progress against the objectives of the implementation of the activities. Special attention will be paid to the analysis of bottlenecks, challenges and risks related to the implementation of the strategy.
- Participating institutions will provide information on the implementation of strategic activities for which they have leading responsibility.
- Low-cost and high-impact objectives should be prioritized above all efforts.

The National Council for Cyber Security is responsible for monitoring the implementation of the Strategy. The Strategy implementation process must be transparent, open and accompanied by democratic oversight.

The Secretariat of strategies maintains all implementation plans and uses them as a basis for progress reporting.

The Strategy will undergo an interim evaluation in 2025 to assess the effectiveness and efficiency of implementation. The final evaluation will be done in 2027.

- Monitoring of activities, which determines whether activities are carried out at the right time and in the right quality. The main tool for monitoring activities is the action plan, which defines the implementation calendar for each activity. Whenever different activities deviate from their schedule, it should be checked whether there are consequences for other activities and resources. The reasons for such deviations should be analyzed, while the implementation plan should be corrected in terms of time.

Monitoring of objectives is based on their indicators. The indicators have the basic value, the intermediate goal and for the last year in accordance with the period of the strategic document. For monitoring to be effective, intermediate goals should be set on an annual basis, becoming part of the annual work plan. The conclusion is then drawn by comparing the actual value with the target goal.

However, the exact definitions and methodologies for calculating the indicators have not been finalized before the adoption of this strategy. So, all the indicators provided in the national cyber security strategy 2023-2027 and its action plan should be considered indicative suggestions. The exact list and description of indicators, their measurement methodology, basic values and objectives will be defined in the Passport of Indicators, which will be finalized within 3 months of the adoption of this strategy.