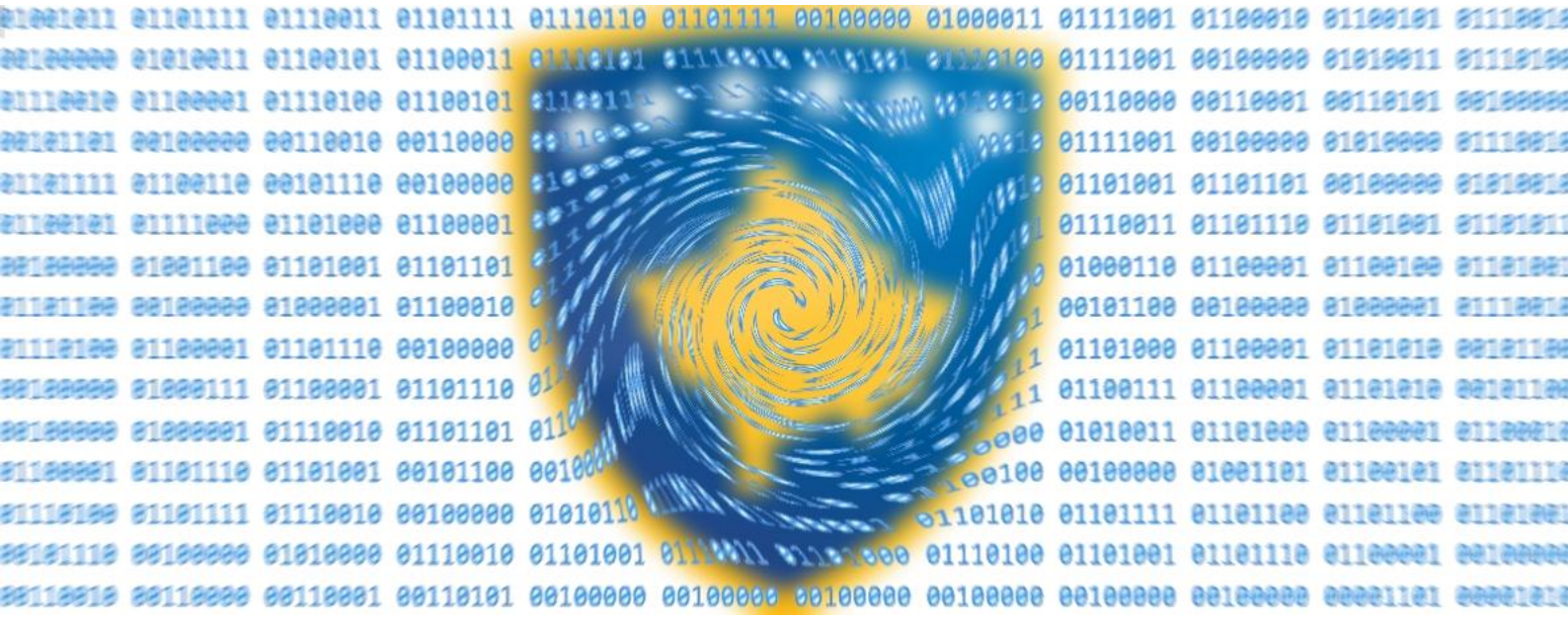
REPUBLIKA E KOSOVËS
REPUBLIKA KOSOVA / REPUBLIC OF KOSOVO

QEVERIA E KOSOVËS
VLADA KOSOVA / GOVERNMENT OF KOSOVO

MINISTRIA E PUNËVE TË BRENDSHME
MINISTARSTVO UNUTRAŠNJIH POSLOVA
MINISTRY OF INTERNAL AFFAIRS



National Cyber Security Strategy and Action Plan 2016 – 2019

December 2015

Executive summary

Today's Internet with its cyber (virtual) space is the largest engineered system ever created by mankind, with billions of connected devices via diverse communication links with billions of users who connect via laptops, tablets, and smartphones. Everyone and everything tends to be connected, and the trend shows its tendency even to increase more. According to Internet World Stats Internet usage growths for period 2000-2014 was 741% and Internet penetration in World level is about 42%. And according to Gartner, Inc. there will be nearly 26 billion devices on the Internet by 2020.With this high usage of Internet, as main business, scientific and social communication platform of a modern citizen, its security and privacy is becoming the main concern.

Internet with its cyber space represents one of the most important drivers of innovation, growth and competitiveness of national economies worldwide. In a globalised and interconnected world, the cyberspace and its security has become one of the key strategic objectives in the area of security of each country. Internet and its cyber space activities, economic, scientific and social, are gaining more and more importance. This online freedom and human values needs to be protected in same manner as in offline world. The digital infrastructure should be protected from incidents, misuse and malicious activities. Governmental bodies should play many roles, in first place they should set clear and transparent guidelines and policies for ensuring not only openness and inclusion for every citizen buts also secure cyberspace.

In Kosovo, the use of Information and Communication Technologies (ICTs) has been spreading rapidly since year 2000 and ICTs are playing important roles in all aspects of our lives. Internet penetration in Kosovo is 76.6%, which is similar to European Union (EU) average and Kosovar habits in cyber space tend to be also similar to global trends. The government organizations, organizations which provide services in critical infrastructure sectors like energy, water resources, health, transportation, communication and financial services have shifted their daily business in Internet. These systems improve the quality and the speed of the services being provided, thus helping organizations work more productively, contributing to the improvement of living standards. But in the same time they are imposed to different threats in the cyber space. These threats are using vulnerabilities inherent in ICTs and may cause denial of service or abuse of service attacks, resulting in potential damage (loss) of human lives, high scale economic losses, disturbance of public order and threats to national security.

In this context the Government of the Republic of Kosovo made a decision nr. 01/30 for drafting the National Cyber Security Strategy 2016 – 2019 and its Action Plan. The working group of all stake holder was established under the Ministry of Internal Affairs (MIA). This working group has mandate to prepare policies, strategies and action plans on ensuring cyber security at the national level. All public organizations and agencies, natural and legal persons, are obliged to perform the duties assigned in the framework of the policies, strategies and action plans determined by the Cyber Security Council.

National Cyber Security Strategy addresses the issue of cyber security in Kosovo through these strategic objectives:

1. Critical information infrastructure protection;
2. Institutional development and Capacity building;
3. Building Public and Private partnership;
4. Incident response;
5. International Cooperation

Contents

1 Introduction 5
1.1 Purpose of the document 5
1.2 Vision 5
1.3 Definitions of terms 6
2 Methodology 9
3 Cyber Security Management System 10
3.1 Strategy Life Cycle 10
3.2 Challenges, Risks, Threats to Cyberspace Security in Kosovo 10
3.3 Addressing cyber crime 12
3.4 Balancing security and privacy 12
4 General Principles 13
5 Legal, Regulatory Framework and Institutional Mechanisms 14
5.1 Legal and regulatory framework 14
5.2 Institutional Mechanisms 15
National Cyber Security Coordinator 15
Secretariat 15
6 Objectives of Cyber Security Strategy 18
6.1 Critical information infrastructure protection 18
6.2 Institutional development and capacity building 19
6.3 Building public and private partnerships 21
6.4 Incident response 21
6.5 International cooperation 22
7 Strategy Implementation, Monitoring and Evaluation 23
7.1 The role of the monitoring system 23
7.2 Institutional Capacities for monitoring and assessment 23
7.3 Indicators for monitoring and evaluation 23
7.4 Monitoring and evaluation instruments 23
8 Action Plan 2016-2019 25

List of Abbreviations

CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
GoK	Government of Kosovo
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
KIA	Kosovo Intelligence Service
KJJ	Kosovo Judicial Council
KSF	Kosovo Security Force
ICT	Information and Communication Technology
MED	Ministry of Economic Development
MIA	Ministry of Internal Affairs
MKSF	Ministry for the Kosovo Security Force
NAPDP	National Agency for Protection of Personal Data
NATO	North Atlantic Treaty Organisation
NCSC	National Cyber Security Council
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Stability and Cooperation in Europe
RAEPC	Regulatory Authority of Electronic and Postal Communications

1 Introduction

1.1 Purpose of the document

The purpose of this document is establish the general foundation about National Cyber Security Strategy for following four years in Republic of Kosovo. Furthermore this document outlines the vision of Government of Kosovo about the cyber security and its corresponding action plan. National Cyber Security Strategy is part of the Government Programme 2015-2018 and linked with the National Plan for the adoption of the Acquis.

In this era of globalization, after the energy the cyberspace security has become one of the key strategic objectives of each country. The digital revolution has been gaining ground in all spheres of life of the modern world. And more than ever, every country is trying to benefit of cyber space by boosting the, economic, scientific, social, and even political development. The development of digital infrastructure such as Internet has heavily changed our social and economic everyday life. The new mental shifting toward this digital infrastructure is happing now.

The online freedom and human values needs to be protected in same manner as in offline world. The digital infrastructure should be protected from incidents, misuse and malicious activities. Governmental bodies should play many roles, in first place they should set clear and transparent guidelines and policies for ensuring not only openness and inclusion for every citizen buts also secure cyberspace.

In 2013 the Kosovo Association of Information and Communication Technology (STIKK) published a study about an Internet Penetration and usage in Kosovo[1]. According to this study the Internet penetration based on households is 84.8%, and based on users is 76.6%, which is similar to European Union (EU) average. Furthermore this study stresses out that most of the Kosovar habits in cyber space are comparable to global trends.

Referring to the "*Analysis of the strategic review of the security sector of the Republic of Kosovo*"[2], cybercrime as unconventional crime has been identified as one of the risks, challenges and global threats that may affect the security of Kosovo.

The Republic of Kosovo is committed to promote stability and security, not only domestically but also be an important contributor to regional and wider security. Therefore international cooperation in the field of cyber security remains a priority for Kosovo.

1.2 Vision

Kosovo will ensure a safe environment of cyber space by minimizing and preventing cyber threats in cooperation with national and international partners.

[1] STIKK - http://www.stikk-ks.org/uploads/downloads/Internet_penetration_and_usage_in_Kosovo.pdf

[2] Analysis - http://www.kryeministri-ks.net/repository/docs/Analysis_of_Strategic_Security_Sector_Review_of_RKS_060314.pdf

1.3 Definitions of terms

At a European and International level, there is a lack of a harmonised definition of "cyber" and "cyber security". The understanding of cyber security and other key terms varies from country to country.

In this chapter will be presented definitions of specific terms compliant with basic meaning of the terms in EU countries. Purpose of the list of the terms is to raise awareness among general population on the cyber terminology.

"Cyber" is defined as: *"anything relating to, or involving, computers or computer networks (such as Internet)"*.

According to International Standardisation Organisation (ISO) "cyber" is *"complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form"*.

Cyberspace

Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.

It is also known as the global environment that is created through the interconnection of communication and information systems. The cyberspace includes the physical and virtual computer networks, computer systems, digital media and data.

Cyber security

In the Cyber Security Strategy of the European Union (An Open, Safe and Secure Cyberspace)[3], "*Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.*"

International Standardisation Organisation (ISO) defines cyber security as *"preservation of confidentiality, integrity and availability of information in cyberspace"*.

Other definitions, define Cyber security as the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Therefore, cyber security in Kosovo is the desired objective of the IT security situation, in which the risks of the Kosovo cyberspace have been reduced to an acceptable minimum. Cyber security (in Kosovo) is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in Kosovo cyberspace. It is also the desired situation in which the protection of cyberspace is proportionate to the cyber threat and the possible consequences of cyber-attacks.

Cyber Crime

According to the above mentioned Cyber Security Strategy of the European Union, *"Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are*

[3] JOIN(2013) 1 final, 7 Feb 2013 - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001

involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)."

It consists of criminal acts that are committed online by using electronic communications networks and information systems. It is a borderless problem that can be classified in three broad definitions[4]:

- Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
- Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.
- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

Cyber attack, cyber espionage and cyber sabotage

A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage.

Cyber defence is mainly used in military context, but it may be also related to criminal and espionage activities. NATO uses the following definition when referring to cyber defence "the ability to safeguard the delivery and management of services in an operational Communications and Information Systems (CIS) in response to potential and imminent as well as actual malicious actions that originate in cyberspace". Cyber Defence consists of following duties: Protect, Detect, Respond, and Recover.

Cyber Intelligence

Activities using all "intelligence" sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-attacks.

Cyber-terrorism is an increasingly attractive choice for terrorists because it can be accomplished with only modest financial resources, with anonymity, and from a great distance. Cyber-terrorism has its greatest potential for damage in conjunction with coordinated physical attacks. The prefix *cyber* is used here because the terrorist attacks or uses technology.

Critical infrastructures

Critical infrastructures are assets or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences.

Green Paper on a European Programme for Critical Infrastructure Protection, the European Commission provides an indicative list of 11 critical sectors:[5]

- Energy
- Information, Communication Technologies (ICT)
- Water

[4] European Commission - http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm
[5] European Commission - Green Paper on a European programme for critical infrastructure protection http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576

- Food
- Health
- Financial
- Public & Legal Order and Safety
- Civil Administration
- Transport
- Chemical and Nuclear Industry
- Space and Research

Critical Information Infrastructure (CII):
ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)
The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Alert
Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Computer Security Incident Response Team (CSIRT)
A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client.

A CSIRT can be a formalized team or an ad-hoc team. A formalized team performs incident response work as its major job function. An ad-hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises.

Computer emergency response teams (CERT)
Computer emergency response teams (CERT) are expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team (CSIRT).

The name "Computer Emergency Response Team" was first used by the CERT Coordination Center (CERT-CC) at Carnegie Mellon University (CMU). The abbreviation CERT of the historic name was picked up by other teams around the world.

European Network and Information Security Agency (ENISA)
The European Network and Information Security Agency (ENISA) is a European Union (EU) agency dedicated to preventing and addressing network security and information security problems.

2 Methodology

National Cyber Security Strategy is designed based on assessments and analysis of law enforcement agencies, government and local and international organizations, global trends and practices and policies of the European Union. In this context, the strategy is in harmony with the instructions of ENISA and strategies of the member states of the EU.

Working Group to draft a Strategy has been formed by the Minister of Interior with the Decision no. 195/2015 dated 05.06.2015 which included all state institutions, professional associations, private sector, civil society and international partners.

At the first meeting of the Working Group an initial smaller group was assigned to develop an initial draft of the Strategy. This sub group held several meetings and developed the initial draft which was forwarded to all members. The strategy was drafted by insuring complete transparency and involvement of all members and representatives of financial institutions.

The strategy was developed by applying comparative method, initially by examining the similarities and differences of cyber security in Kosovo with other regional states and other countries. Based on this analysis, current and future measures to be taken have been identified to create an effective mechanism and in line with global trends to ensure cyber security in Kosovo.

Theoretical literature and empirical studies in the field of cyber security have been analysed and used as primary and secondary sources: such as analysis and risk assessments from various institutions, publications from national and international organisations, the strategies adopted by EU member states, ENISA's guidelines and other relevant documents.

Between October 21-23 workshop has been held in Boge, supported by the EU Funded Project ENCYSEC, where all institutions of the working group were invited. All representatives had the opportunity to offer their proposals and discuss the activities of the Strategy and Action Plan.

3 Cyber Security Management System

3.1 Strategy Life Cycle

Based on the key recommendations of international bodies (NATO, ENISA), National Cyber Security Strategy should be developed within the life cycle, which should include the following stages:

1. Development,
2. Implementation,
3. Evaluation,
4. Adaptation of the strategy.

This way will ensure continued progress of strategy, procedures and products, and in accordance with changed circumstances in immediate and wider environment.

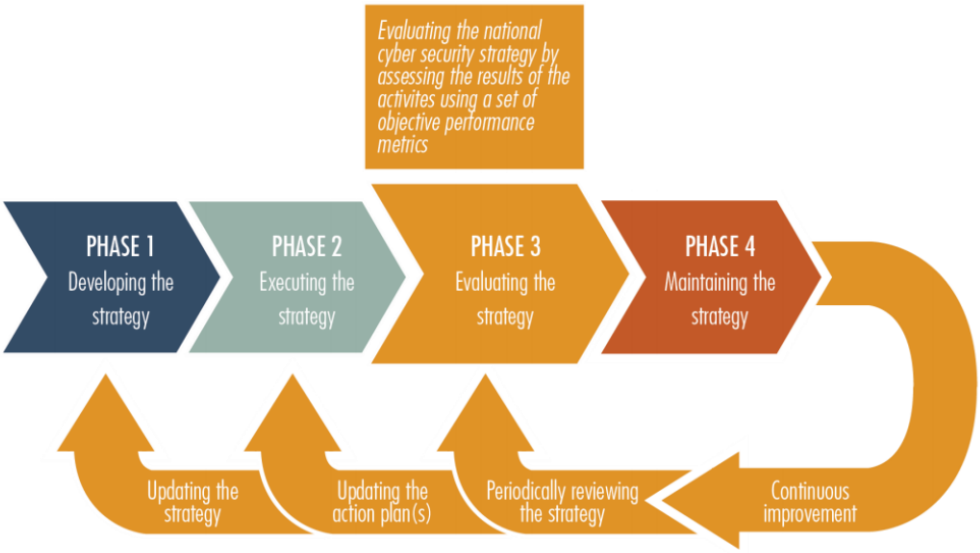


Figure 1: Cyber Security Lifecycle (Source: ENISA, 2012)

3.2 Challenges, Risks, Threats to Cyberspace Security in Kosovo

TKIAng into consideration that cyber space is a space of criminal misuse, there are number of risks and threats where the security and safety of people in cyber space is exposed to.

Many of the risks and impacts of cyber incidents are shared between governments and the private sector. Our aim is to mitigate cyber security risks and not tolerate those with a very high impact risks.

With the current know-how, the primary threats and risk elements related to ICT systems in the Republic of Kosovo are listed below;

Threats

Cyber threats take place from the possibilities and intentions of an enemy to launch a cyber-attack on the Communication and Information Systems.

There are five kinds of cyber-attacks motivated by:

- **Revenge, Curiosity:** Performed by insiders and script-kiddies
- **Monetary Gain:** Performed by organised Crime
- **Espionage, Activism:** Cyber-attacks involving unnoticed intrusion of a third party into a Communication and Information Systems to read, change, delete or even add information (intrusion). Such intrusions can also be used to make improper use of the Communication and Information Systems attacked to, for instance, attack other systems.
- **National Security:** Performed by state sponsored actors
- **Terrorism:** Cyber-terrorism involves highly targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage. While we'd often associate terrorism with loss of life, we cannot overlook important results like 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, organize terrorist actions, and thus pose a threat to national security of the Republic of Kosovo.

Nowadays critical information infrastructures are more frequently becoming the target of increasingly complex cyber attacks. Such attacks are specifically aimed at particular targets by terrorists and hackers looking for sensitive information or with the aim to destroy this critical information infrastructure.

Risks

- Absence of National Cyber Security Council with its functions
- Non listing of a National and other CERTs in Trusted Introducer[6] and FIRST[7]
- Lack of knowledge and understanding of the digital attack possibilities, poses a real risk.

Vulnerabilities

- ✓ There is no complete security and protection in the cyber domain. However, the chance of a cyber-attack is much greater than that of a physical attack. The authorities and ordinary citizens of Kosovo have already been the victim of a cyber-attack, and will certainly be facing cyber-attacks in the near future, with limited success.
- ✓ One of the biggest challenges lies in raising awareness among personnel as most of them use cloud computing and social media technologies as well as portable memory devices (e.g. thumb drives, USB flash drives). According to the world statistics, most cyber incidents are caused by human error. As a result, the "internal" threat is real as well.
- ✓ Despite the limited direct impact, the risks related to cyber-attacks should certainly not be underestimated.

[6] Trusted Introducer List of CERT/CSIRT- https://www.trusted-introducer.org/directory/country_LICSA.html
[7] FIRST listed Members - https://www.first.org/members/teams

3.3 Addressing cyber crime

There is an urgent need for a close cooperation between law enforcement authorities worldwide in order to fight the rapid growth of cybercrime.

Cybercrime continue to pose the most significant challenges for the Republic of Kosovo institutions in general and in particular to the Kosovo Police. The Republic of Kosovo has taken concrete steps in establishing the legal infrastructure to prevent and combat all forms of cybercrime, but still many challenges remain, especially in technical terms to deal successfully with this form of criminality, which in Kosovo is a relatively new phenomenon.

Significant growth of Internet users in recent years in Kosovo has brought with it increased danger of computer crime and cyber-attacks. Although so far there have been no cases of serious penetration and damage to systems with state data, various criminal activities were enough to highlight the weaknesses of computer networks in Kosovo, which is still considered in the development stage.

According to data available, main target of computer attacks in Kosovo so far they have been user accounts, banking system and websites.

The capabilities of law enforcement agencies, Kosovo Police (Cybercrime Unit) in combating cyber crime, also with regard to protection against espionage and sabotage, must be strengthened. There is a need to reinforce the personnel of individual cybercrime police departments by modernising their technological equipment, supporting their international cooperation in information sharing and training. In addition there is a need in providing professional education and training to police specialists by creating multidisciplinary academic environment in order to enhance Kosovo Police capacities in cybercrime prosecution.

Cybercrime requires a specialized response of criminal justice authorities. Law enforcement authorities and prosecution should be able to conduct investigations and prosecute offences against computer data and systems, offences committed over computers, as well as electronic evidence material relating to any criminal offence.

3.4 Balancing security and privacy

In accordance with the Constitution of the Republic of Kosovo the public and private authorities shall guarantee the observance of basic rights and liberties. Basic rights must also be guaranteed in cyber space Increased cyber security may improve, for instance, the protection of the privacy and property of network users.

Government of the Republic of Kosovo will adopt necessary measures to protect and guarantee national cyber security. These measures will respect privacy, fundamental rights and liberties, free access to information and other democratic principles.

4 General Principles

The structure and contents of this document are based on the following guiding principles:

Principle of Constitutionality and Legality – Actions undertaken in order to enhance cyber security must be based on the provisions provided for in the Constitution of the Republic of Kosovo, legislation in force and international agreements.

Principle of National Security – Cyber security is an integral part of national security, it supports the functioning of the state and society, the competitiveness of the economy and innovation. This principle mean ensuring the right to security and protection for all citizens through cybercrime prevention.

Principle of Subsidiarity – Because of the diverse ownership and operation of various ICT systems, the State cannot assume sole responsibility for protecting cyberspace and the rights of citizens online. The owners and operators of information and communication technology are primarily responsible for protecting their systems and the information of their customers.

Principle of Holistic Approach - It is crucial need for development of holistic approach to face threats in cyberspace,

Principle of Public and Private Partnership - Cyber security is ensured in a coordinated manner through cooperation between the public and private sectors, tKIAng into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace.

Principle of continuity – Activities should be seen as a part of a continuous strategy. This is especially important because administrative/procedural and time limits will be imposed, and because different initiatives and activities will need to be linked with actions that will continue for several years.

Principle of Confidentiality - Institutions with responsibility to prevent and combat cybercrime should seek to establish trust in protecting investigation, data and information integrity from misuse by those with access to them.

Principle of Human Rights and Freedoms - Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity regardless of ethnicity, gender, age, religion throughout all stages.

Principle of International Cooperation - Cyber security is enhanced via international cooperation with international partners and allies. Through cooperation, Kosovo will play a substantial role in promoting global cyber security and at the same time enhancing its own competences.

5 Legal, Regulatory Framework and Institutional Mechanisms

5.1 Legal and regulatory framework

In the field of Cyber Security, the Republic of Kosovo has in effect a wide legislative ground, where as a primary legislation can be mentioned, but not limited to:

- ✓ Constitution of the Republic of Kosovo[8]
- ✓ Law No. 03/L-050 on the establishment of the Kosovo security council[9]
- ✓ Law No.03/L –166 on prevention and fight of the Cyber Crime[10]
  Law No. 04/L-145 on Information society government bodies[11]
- ✓ Law No. 04/L-094 on the information society services[12]
- ✓ Law No. 04/L-109 on electronic communications[13]
- ✓ Law No. 05/L-030 on interception of Electronic communications[14]
- ✓ Law No.03/L – 172 on the protection of personal data[15]
  Law no. 04/L-076 on Police[16]
- ✓ Law no. 03/L-142 on Public Peace and Order[17]
  Law no. 03/L063 on Kosovo Intelligence Agency[18]
- ✓ Law no. 04/L-149 on the Execution of Penal Sanctions[19]
- ✓ Law No. 04/L-065 on copyright and related rights[20]
- ✓ Law no. 03/ L-183 on the Implementation of International Sanctions[21]
- ✓ Law no. 04/L-213 on International Legal Cooperation in Criminal Matters[22]
- ✓ Law no. 04/L-052 on International Agreements[23]
- ✓ Law no. 04/L-072 on Controlling and Supervising State Borders[24]
- ✓ Law no. 04/L-093 on Banks, micro finance Institutions and Non Bank Financial Institutions[25]
- ✓ Law No. 04/L-064 on Kosovo agency on forensic [26]
- ✓ Law No. 04/L-198 on the trade of strategic goods; [27]
- ✓ Law No.04/L –004 on private security services;[28]
- ✓ Law No. 03/L-046 on the Kosovo security force;[29]
- ✓ Code No. 03/L-109 customs and excise code of Kosovo; [30]
- ✓ Law No. 04/L-099 on amending and supplementing customs and excise code in Kosovo no. 03/l-109[31]
- ✓ Law No.03/L –178 on classification of information and security clearances[32]

[8] Constitution of the Republic of Kosovo - http://www.kushtetutakosoves.info/repository/docs/Constitution.of.the.Republic.of.Kosovo.pdf
[9] Law No. 03/L-050 - http://www.kuvendikosoves.org/common/docs/ligjet/2008_03-L050_en.pdf
[10] Law No.03/L –166 - http://www.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf
[11] Law No. 04/L-145 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20information%20society%20government%20bodies.pdf
[12] Law No. 04/L-094 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20information%20society%20services.pdf
[13] Law No. 04/L-109 - http://www.kuvendikosoves.org/common/docs/ligjet/109%20Law%20on%20Electronic%20Communications.pdf
[14] Law No. 05/L-030 https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968
[15] Law No.03/L – 172 - http://www.kuvendikosoves.org/common/docs/ligjet/2010-172-eng.pdf
[16] Law no. 04/L-076 - http://www.kosovopolice.com/repository/docs/Law_on_Police.pdf
[17] Law no. 03/L-142 - http://www.kuvendikosoves.org/common/docs/ligjet/2009-142-eng.pdf
[18] Law no. 03/L063 - http://www.assembly-kosova.org/common/docs/ligjet/2008_03-L063_en.pdf
[19] Law No. 04/L-149 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20execution%20of%20penal%20sanctions.pdf
[20] Law No. 04/L-065 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20copyright%20and%20related%20rights.pdf
[21] Law no. 03/ L-183 - http://www.kuvendikosoves.org/common/docs/ligjet/2010-183-eng.pdf
[22] Law No. 04/L-213 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20international%20legal%20cooperation%20in%20criminal%20matters.pdf
[23] Law No. 04/L-052 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20international%20agreements.pdf
[24] Law No.04/L-072 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20state%20border%20control%20and%20survailance.pdf
[25] Law no. 04/L-093 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20banks,microfinance%20institutions%20and%20NFI.pdf
[26] Law No. 04/L-064 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20Kosovo%20Forensic%20Agency.pdf
[27] Law No. 04/L-198 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20the%20trade%20of%20strategic%20goods.pdf
[28] Law No.04/L –004 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20private%20security%20services.pdf
[29] Law No. 03/L-046 - http://www.kuvendikosoves.org/common/docs/ligjet/2008_03-L046_en.pdf
[30] Code No. 03/L-109 - http://www.kuvendikosoves.org/common/docs/ligjet/2008_03-L-109_en.pdf
[31] Law No. 04/L-099 - http://www.kuvendikosoves.org/common/docs/ligjet/Law%20on%20amending%20customs%20and%20excise%20code.pdf
[32] Law No.03/L –178 https://gzk.rks-gov.net/ActDetail.aspx?ActID=2690

- ✓ Law No. 03/L-122 on foreign service of the Republic of Kosovo[33]

- ✓ Code No. 04/L-082 criminal code of the Republic of Kosovo[34]
- ✓ Criminal No. 04/L-123 procedure code[35]
- ✓ Code No. 03/L-193 juvenile justice code[36]
- ✓ Regulation No. 18/2011 on the distribution and transfer of classified information[37]

This strategy is in compliance with the international acts that regulate the field of Cyber Security, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013)[38], ENISA Guidebook on National Cyber Security Strategies (2012)[39], Cyber Security Strategies of other EU Countries.

5.2 Institutional Mechanisms

The institutional mechanism concerns the role and coordination of activities of main stakeholders which have a role on cyber security in Kosovo.

National Cyber Security Coordinator

National Cyber Security Coordinator is Minister of Internal Affairs or his authorized person, and is responsible and mandated to coordinate, guide, monitor and report on the implementation of policies, activities and actions in connection with the National Cyber Security Strategy.

Secretariat

Secretariat is a body established, with a function to collect information and data from other institutions, analyse and assess gathered information, and develop analytical reports for National Coordinator and National Cyber Security Council. In addition Secretariat will disseminate timely information to all appropriate stakeholders, supporting national action plan for Cyber Security;

Ministry of Internal Affairs

MIA has a functional role in achieving the objectives set out in this strategy. Kosovo police as law enforcement agency within MIA, has full authority in combating all forms of cybercrime.

MIA has the leading role in coordinating the strategy, monitoring the implementation of the Action Plan and for drafting periodic reports. MIA is also responsible for the formulation and monitoring of policies and legislation in the field of general security and cyber security. Kosovo police as the law enforcement agency within the Ministry of Interior, has the main responsibility in combating all forms of cybercrime, through the Department for Cyber Crime and other supporting structures within the Kosovo Police. Kosovo Police also will serve as point of contact 24/7 for international cooperation in the field of cybercrime.

The Kosovo Judicial Council,

Ensures that the Kosovo courts are independent, professional and impartial, in order for the judicial system to be more efficient in the fight against cybercrime.

Kosovo Prosecutorial Council,

[33] Law No. 03/L-122 https://gzk.rks-gov.net/ActDetail.aspx?ActID=2615
[34] Code No. 04/L-082 http://www.kuvendikosoves.org/common/docs/ligjet/Criminal%20Code.pdf
[35] CRIMINAL No. 04/L-123 PROCEDURE CODE - http://www.KJC-ks.org/repository/docs/Kodi_procedures_penale_(anglisht)_878084.pdf
[36] Code No. 03/L-193 http://gzk.rks-gov.net/ActDetail.aspx?ActID=2698
[37] Regulation No. 18/2011 http://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=10554
[38] Cybersecurity Strategy of the European Union http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[39] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Ensures that the prosecution system in Kosovo is independent, impartial and professional in exercising the pursuit, investigation and detection of cyber crime offenses and represents indictments before courts on behalf of the state.

Prosecution and Courts
Are the institutions responsible for prosecuting perpetrators, their adequate punishment, confiscation of property and assets gained through criminal activities

Secretariat of the Kosovo Security Council
Secretariat, as integral part of the Security Council of Kosovo is preparing periodic reports and analysis for the Government of the Republic of Kosovo and Security Council of Kosovo dealing with political issues of security and provides assistance in drafting security policies in Kosovo, including capacity building, policy and research instruments, providing administrative and functional support for the Kosovo Security Council.

Kosovo Intelligence Agency
KIA identifies threats endangering security in Kosovo. Threat to the security of Kosovo is considered a threat to the territorial integrity, institutional integrity, constitutional order, stability and economic development, as well as global security threats against Kosovo.

Ministry of Justice
MJ prepares and develops legislation in the field of justice, coordinates and develops international judicial cooperation in criminal matters.

Ministry for the Kosovo Security Force
MKSF develops and strengthens cyber security of communications and information systems for MKSF/KSF, systems that are used for performing tasks in accordance with the constitutional mission. KSF may engage in support of civil authorities in the protection of data and critical infrastructure in the event of a crisis in the country.

Ministry of Economic Development
Ensures quality of service and technical standards in the field of telecommunications, develop policies to promote competition in the telecommunications field, examines the needs and requirements of customers in the telecommunications, supports information technology and innovations, supports access to technology to all citizens of Kosovo and encourage the development of training systems information technology.

Ministry of Finance
MF through Customs, the Financial Intelligence Unit and the Tax Administration, will help in strengthening cyber security, prevent and combat cybercrime.

Ministry of Education, Science and Technology
MEST plays important role in the prevention and awareness raising through the development of curricula, organising of awareness-raising activities for the use of the Internet and other extra-curricular activities.

Ministry of Foreign Affairs
MFA has a role in terms of providing assistance to international cooperation in the fight against organized crime

Ministry of European Integration
MEI provides that legal framework and policies of the Government of the Republic of Kosovo are in accordance with the legislation and policies of the EU.

Regulatory Authority of Electronic and Postal Communications
RAEPC is a regulatory body, which implements and monitors the regulatory framework defined by the law on Electronic Communications, the Law on postal services, and the development policies in the field of electronic communications and postal services

Agency for Information Society
AIS makes the coordination, management and monitoring of the processes and mechanisms of electronic governance in relation to ICT infrastructure, expansion of Internet services and content websites in the institutions of the Republic of Kosovo, accumulation, management, dissemination and storage of data, by creation of the national electronic data centre, and by providing safety and protection of electronic communications infrastructure and data. AIS as appropriate, helps relevant institutions in combating cybercrime and ensures the protection of personal data in electronic form, in accordance with the legislation in force.

National Agency for Protection of Personal Data
NAPDP ensures that controllers comply with their obligations on the protection of personal data and that data subjects are informed about their rights and obligations in accordance with the Law on Protection of Personal Data. It also provides advice to the Assembly of Kosovo, the Government, local authorities and all holders of public authority in Kosovo regarding the issues on the Protection of Personal Data, as well as advising all private institutions concerning the Protection of Personal Data.

6 Objectives of Cyber Security Strategy

In the framework of its National Cyber Security Strategy, Republic of Kosovo pursues the following strategic objectives:

1. Critical information infrastructure protection
2. Institutional development and capacity building
3. Building public and private partnerships
4. Incident response
5. International cooperation

6.1 Critical information infrastructure protection

This Strategy aims to establish a safe electronic environment in the Republic of Kosovo, with specific considerations and actions for the protection of critical information infrastructures, whose disruption or destruction would have severe consequences to vital societal functions.

The protection of critical information infrastructures is the main priority of cyber security. The public and the private sector must create an enhanced strategic and organizational basis for closer coordination based on intensified information sharing. Where necessary and in case of specific threats protective measures have to be made mandatory. Furthermore we will examine the necessity of harmonizing rules to maintain critical infrastructures during IT crises.

6.1.1. Identification of Critical Information Infrastructures

It is necessary to identify and assess the truly *critical* infrastructures within the Republic of Kosovo and to target them for the best possible protection. These critical infrastructures will be identified and assessed based on a number of predetermined criteria. ENISA *methodologies for the identification of Critical Information Infrastructure assets and services*[40] will be taken into consideration.

The steps that will be followed for the identification of critical information infrastructures will include the following:

- **Determination of services** that will be targeted (e.g. voice communications, data communications, data storage, data processing), that could be classed as critical,
- **Identification of infrastructures** that are technically indispensable for the operation of these services,
- **Introduction of objective criteria** for the level of protection that each infrastructure element needs, with categorisation of infrastructures and the use of criteria such as the number of affected users, the sensitivity level of the information that is concentrated, stored, transmitted or processed on these infrastructures, etc.
- **Check the criteria** with the development of scenarios that consider the disruption of operation of selected infrastructure, within the bounds of regular exercises.

[40] ENISA https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis

6.2 Institutional development and capacity building

6.2.1 Appointment of the National Coordinator and the duties of the National Cyber Security Council

Since there is a multi-stakeholder approach to security measures, it is very important to understand and accept that maintenance of acceptable levels of security in the "cyber space" can be accomplished only via cooperation between the different stakeholders involved, within a framework of coordinated response to the various threats that have already been mentioned in Chapter 3.

Coordination of the competent or relevant governmental authorities is absolutely necessary. This coordination activity is productive when performed by an entity which is in a position to organise and coordinate the various actors and actions of the Republic of Kosovo for correct response to the threats that are around today, as well as rising and new threats in cyberspace.

National Cyber Security Council should be established to strengthen cooperation within the government and with the private sector and provide recommendations at high political levels on strategic issues.

Council should be comprised of representatives of following institutions: Ministry of the Internal Affairs, Kosovo Police, Kosovo Forensics Agency, Ministry of Kosovo Security Forces, Kosovo Intelligence Agency, Agency of Information Society, Kosovo Security Council, Ministry of Justice, Kosovo Prosecutorial Council, Kosovo Judicial Council, Ministry of Finance, Kosovo Customs, Ministry of Education, Science and Technology, Ministry of Foreign Affairs, Regulatory Authority of Electronic and Postal Communications, Central Bank of Kosovo. On specific occasions additional ministries and agencies will be included.

Business representatives will be invited as associated members. Representatives from academia will be involved, on a technical level. The National Cyber Security Council is intended to coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector.

6.2.2 Capacity building for the Strategy Secretariat

In order to ensure monitoring and coordination of activities of the Strategy it is necessary to recruit an official in the Secretariat of the Strategy. Ministry of Interior until to the third quarter of 2016 will end all recruitment procedures of hiring a responsible official for this task.

In addition, with the support of the international partners training and study visits will be organised in order to increase the capacity of the official in charge.

6.2.3 Awareness raising

We will work to promote a culture of cyber security across society, including through cooperation with the education system, with industry and through the promotion of events like "European Cyber Security Month". Special focus should be on government employees, new generations, as well as on end-users of the Internet and continuous introduction of new programmes on information security at all levels of education with a view to use advanced information systems.

Necessary measures should be taken in place in order to facilitate:

- Management of expertise and knowledge in the cyber domain. Flexible adjustment of necessary training in relation to a fast and constantly changing threat.
- Participation in national and international exercises, training events (workshops, courses, etc.). Conduct a program of cyber security exercises to test and refine event response arrangements. Domestic and international cyber security training exercises play an important role in the development and assessment of cyber security capabilities.
- Awareness tools (e.g. e-learning) and information campaigns have to be set up for all citizens of Kosovo
- Adequate courses for all stakeholders (as needed, in time): in-house, outsourced, in national and international partnership (e.g. by participation in various training activities) It is also important that the executives in the organisation have sufficient understanding of the cyber domain. Therefore, cyber aspects have to be integrated into the existing curricula of education in Kosovo.

6.2.4 Legal infrastructure

The main goal is to harmonize the legal framework with the European Union. In this context, in 2016 Law on Identification and Protection of Critical Infrastructure will be drafted. An important part of this Law shall be the Critical Information Infrastructure Protection (CIIP).

Furthermore, it was identified as necessary to review the Law on Preventing and Combating Cybercrime, and draft od the necessary bylaws which cover the area of cyber security.

The legal framework will be amended and harmonized under the National Plan for the Implementation of the Stabilisation and Association Agreement.

6.2.5 Human capacity building

In order to harmonize the activities and training of all institutions involved in this Strategy, training curriculas will be developed. The main purpose is to organize training, in order to improve coordination and cooperation between the institutions involved, but training will be organized specifically for one or group of institutions.

The important part is to design scenarios and holding joint exercises, through which the institutions involved will test their capacity in response to the various challenges. Organising these exercises will improve capacity in incident response to different threats, whether at the national level and institutional.

6.2.6 Technical Infrastructure building

Technical infrastructure plays an important role in strengthening cyber security in Kosovo and all the institutions involved are committed in advancing their information technology systems.

Among other things, RAEPC (RAECP) will establish a platform for receiving and recording of cyber incidents and Kosovo Police will advance equipment for the investigation of cybercrime.

6.2.7. Foster research and development

Republic of Kosovo will continue and intensify research on IT security and on critical infrastructure protection. Research and Development Capabilities will be developed within Kosovo and they will also be used for the participation in national and international projects according to the resources available.

Research and development is a key component in improving Kosovo's response to cyber security threats.

6.3 Building public and private partnerships

6.3.1 Increase cooperation with the private sector

Since most of the Critical Information Infrastructure belongs to the private sector it is necessary to define a clear cooperation with private sector in the field of cyber security.

In particular, to define procedures on information exchange with:

- Internet Service Providers
- Banking sector
- Electric Power
- Water Supply
- Transport (Air and Ground)
- Academia

Joint activities for education on cybersecurity will be organised, which will focus on giving advice about the cyber security curriculum, in relation to the certification of information security experts and the further development of learning modules.

6.4 Incident response

6.4.1 Functionalisation of a National CERT/CSIRT and creation of other CERT/CSIRT-s in Kosovo

TKIAng into consideration that security preparedness is best achieved by early warning and prevention, the Incident Response Centres will submit recommendations to the Secretariat of the Authority both on a regular basis and for specific incidents. If the cyber security situation reaches the level of an imminent or already occurred crisis, the National Cyber Security Centre will directly inform the National Cyber Security Authority headed by the National Cyber Security Coordinator or his authorized person.

Ensuring the full functionality of Computer Emergency Response Teams (CERTs/CSIRTs) within Kosovo is an integral and vital part of this Strategy, and also of meeting our commitments of the Kosovo Government. The main functions of CERTs/CSIRTs are the prevention of serious incidents related to network and information security, as well as the immediate and appropriate response to such incidents when they occur.

It is emphasized that for the correct operation of a CERT/CSIRT, the following are required:

- necessary infrastructure, and
- staffing with appropriately trained (to a very high level) personnel.

Policy should cover the very practical steps that an organization needs to take when a cyber security incident occurs. Documented incident handling tasks are aimed first at securing information assets – minimizing damage -- as quickly as possible. Beyond providing immediate, on-the-scene protection, written incident-handling tasks will strengthen organizational learning and may assist the cyber security professional in the pursuit and prosecution of criminals. It is always a good idea to practice incident handling and continually update procedures so that when these are needed in live situations they will be proven and reliable.

6.4.2 Listing and accreditation of CERT/CSIRT-s in Trusted Indroduced and First

Detailed explanations of how to become listed in **Trusted Indroduced**[41] **and First**[42] is available in their websites. Becoming a listed team is a mandatory requirement and first step in order to become accredited and thereby getting access to the member's only services.

6.5 International cooperation

6.5.1 Organisation and participation in international events

Kosovo Government is pursuing an active approach to international engagement on cyber security through:

- bilateral or multilateral agreements with key allies and other like minded nations to strengthen
  cooperation on cyber security
- regional forums, with a focus on capacity building initiatives within our region
- international organisations to help promote international best practice and develop and foster a
  coordinated global approach to combating cyber security threats, including spam.

6.5.2 Enhancing international cooperation

In global cyberspace security can be achieved only through coordinated tools at national and international level. Kosovo will play an active role in international cooperation at European and global level, particularly by exchanging information, formulating international strategies, developing voluntary schemes and legally binding regulations, prosecuting criminal cases, holding transnational exercises and conducting cooperation projects.

At EU level we support appropriate measures based on the action plan for the protection of critical information infrastructures, the extension and moderate enlargement of the mandate of the European Network and Information Security Agency (ENISA) in view of the changed threat situation in ICT and the pooling of IT competences in EU institutions. Kosovo aspires to join EU in the future and as such will try to establish contacts with ENISA.

We will shape our external cyber policy in such a way that national interests and ideas concerning cyber security are coordinated and pursued in international organizations, such as ENISA, the OSCE, the Council of Europe, the OECD and NATO. Kosovo will give the best contribution in the anti-botnet activities worldwide.

[41] https://www.trusted-introducer.org/processes/registration.html

[42] https://www.first.org/membership/process

7 Strategy Implementation, Monitoring and Evaluation

7.1 The role of the monitoring system

The implementation process of the strategy will involve the achievement of strategic objectives, specific objectives and activities. Monitoring and evaluation of the results of implementation efficiency objectives and relevant activities, will constitute an integral part of Strategy process and key components to its delivery. Monitoring and Evaluation will provide the means to measure progress in relation to the stated objectives, to assess the need to establish management rules, in particular the activities. The monitoring process will be done by institutions with broad participation from stakeholders.

The main dimensions of strategy monitoring and evaluation are:

- Institutional capacity;
- Monitoring indicators during and at the end of the four year period;
- Information sources and measuring instruments;

7.2 Institutional Capacities for monitoring and assessment

Monitoring and evaluation system will be extended to all institutions responsible for the realisation of the objectives set in the Strategy and Action Plan.

- National Cyber Security Coordinator as the leading institution for achieving objectives shall monitor the most important indicators related to Cyber Security. At the end of every year, will prepare a progress report on the objectives.
- Ministries and other institutions specified in action plan will be responsible for monitoring and evaluation of activities that have been allocated to these ministries or their subordinate institutions. These institutions will submit periodic reports to the National Cyber Security Coordinator, in order to be unified reports.
- Non-Governmental Organizations will participate in the monitoring and assessment process of the strategy being part of the round tables organized by the National Cyber Security Strategy Coordinator. In these round tables, the non-governmental organizations and civil society will present their observations related to the anti-trafficking projects and programs they have implemented.

7.3 Indicators for monitoring and evaluation

- Number of relevant laws and regulations, which entered into force after the adoption of the strategy;
- Structures established (Coordinator, Secretariat)
- Number of trained staff on Cyber Security per relevant institutions
- Curriculum areas and textbooks that address the issue of Cyber Security
- Number of projects and programs on Cyber Security
- Number of monitoring and evaluation reports on National Cyber Security Strategy
- Number of International activities on Cyber Security.

7.4 Monitoring and evaluation instruments

- Administrative/statistical data of relevant Cyber Security stakeholders
- Progress report

- Surveys regarding the Kosovo citizen's level of knowledge as a result of the conducted cyber security awareness campaigns.

8 Action Plan 2016-2019

The Action Plan reflects its compliance with the framework of the Strategy and is designed within the overall strategic framework defined by the National Cyber Security Strategy.

The Action Plan will be reviewed at the end of each year in order to ensure the viability of the Strategy and harmonization with national and international trends.

The Action Plan for the implementation of this strategy shall include:

- Strategic objectives;
- Specific objectives;
- Concrete activities for the implementation of objectives;
- Determines the responsible and supporting institutions for achieving each objectives;
- Specifies the time frame for the implementation of each objective;
- Determines the necessary financial sources for the development of activities;
- Determines the indicators for the implementation of each objective and activity.

NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2016 - 2019						
Strategic Objective 1 **Critical Information Infrastructure Protection**						
1.1	**Specific Objective: Critical Information Infrastructure Protection**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
1.1.1	Identification of the Critical Infrastructure and Critical Information Infrastructure	K4 2016	Budgeted cost	Ministry of Internal Affairs	Relevant Institutions and international partners (US Embassy, ICITAP, UNDP, ENCYSEC)	List with the Critical Information Infrastructure drafted
1.1.2	Functionalization of the Disaster recovery for data centers in relevant institutions	2016-2019	Budgeted cost	Public and Private Institutions	International Partners	Functionalized centers as per list of identified institutions in activity 1.1.1
1.1.3	Implementation of critical security controls on data networks KSF	2016-2019	Budgeted cost	Ministry of Kosovo Security Forces	Relevant Institutions and international partners	Number of controls conducted
1.1.4	Creating a system for network and information Security	2017-2018	Budgeted cost	Ministry of Kosovo Security Forces	Relevant Institutions and international partners	System created

	of COMSEC / INFOSEC					
1.1.5	Implementation of Security Communication System for the Ministry of Foreign Affairs and Diplomatic Missions	2016-2019	Budgeted cost	Ministry of Foreign Affairs	Relevant Institutions and international partners	System installed in the diplomatic missions
1.1.6	The establishment and functioning of microwave network in MKSF	2016	Budgeted cost	Ministry of Kosovo Security Forces	KP	Network is functionalized
1.1.7	Implementation of the System for Cyber Threat Prevention in Kosovo Police	2016-2017	300,000 €	Kosovo Police	Relevant Institutions and international partners	System is functionalized
1.1.8	Implementation of the System for Cyber Threat Prevention in Kosovo governmental institutions	2016-2019	800,000 €	Agency for Information Society	Relevant Institutions	System is functionalized
1.1.9	Advancement of the technology in KFA with the AFS system	2016-2017	803,537 €	Kosovo Forensics Agency	International Partners	System is functionalized
1.2	**Specific Objective: Develop a business continuity plan for the Disaster Recovery Centers**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
1.2.1.	Development of Business Continuity	K2 2016	Budgeted cost	Ministry of Internal Affairs	Relevant institutions	Plan is drafted

	Plan for Disaster Recovery Centre in Ministry of Internal Affairs					
1.2.2	Implementation of Business Continuity Plan for Disaster Recovery Center	K3 2016	Budgeted cost	Ministry of Internal Affairs	Relevant Institutions	Plan is implemented
1.2.3	Maintenance of Disaster Recovery Centre	K2 2016	Budgeted Cost	Ministry of Internal Affairs	Relevant Institutions	Contract for maintenance is signed
Strategic Objective 2 Institutional development and Capacity building						
2.1	**Specific Objective: Designation of the National Coordinator and the duties of the National Cyber Security Council**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
2.1.1	Decision of the National Coordinator for establishment of hte NCSC	K1 2016	Administrative Cost	Ministry of Internal Affairs	Relevant Institutions	Decision is signed
2.1.2	Organisation of periodical meetings of the NCSC on 3 months basis	2016-2019	Budgeted cost	National Coordinator	Relevant Institutions and International partners, ICITAP, ENCYSEC, UNDP, OSCE	Number of meetings conducted
2.1.3	Drafting of periodical reports	Every 3 months	Budgeted cost	National Coordinator	Relevant institution and international partners	Number of drafted reports

2.1.4	Review of the Action Plan	K4 2016 K4 2017 K4 2018	Donation (OSCE)	National Coordinator	Relevant institutions and international partners (OSCE, ENCYSEC, ICITAP, EU, UNDP)	Action plan revised
2.2	**Specific objective: Capacity Building for the Secretariat of the Strategy**					
No.	**Activity**	**Time Frame**	**Budget**	**Owner**	**Support Institutions**	**Performance Indicators**
2.2.1	Description of duties and responsibilities for the Officer responsible for implementing the Cyber Security Strategy	K1 2016	Administrative cost	Ministry of Internal Affairs	MPA, MF	Position is approved
2.2.2	The announcement of the job advert and recruitment of the officer in charge	K3 2016	Budgeted Cost	Ministry of Internal Affairs	MPA, MF	Official is recruited
2.3	**Specific Objective: Awareness raising**					
No.	**Activity**	**Time Frame**	**Budget**	**Owner**	**Support Institutions**	**Performance Indicators**
2.3.1	Publication of bulletins on the cyber security situation	2016-2019 .	Budgeted cost	National Coordinator	Relevant institutions and international partners(ICITAP,	Published bulletins

					ENCYSEC, UNDP, OSCE)	
2.3.2	Organizing of awareness campaigns	2016-2019	Donation	National Coordinator	Relevant institutions and international partners(ICITAP, ENCYSEC, UNDP, OSCE)	Number of organized campaigns, lectures held, distributed leaflets
2.3.3	Update of the current ICT curricula in pre-university level with cyber security modules	2016-2017	Administrative Cost	MEST	National Coordinator and relevant institutions	Curricula's' are updated
2.3.4	Organization of the European Cybersecurity Month	2016-2019	Donation	National Coordinator	Relevant institutions and International Partners (ICITAP, ENCYSEC, UNDP, OSCE)	Marking the European Cyber Security month
2.3.5	Organization of seminars, conferences, etc.	2016-2019	Donation (OSCE)	National Coordinator	Relevant institutions and International Partners (ICITAP, ENCYSEC, UNDP, OSCE)	Seminars and conferences are organized
2.3.6	Raising awareness and cooperation with parents as well as organizing visits and workshops for parents and	2016-2019	Administrative Cost	MEST	MKRS, MIA, NGO-s, International partners	Workshops organized, visits conducted

	children about the online risks					
2.3.7	Inclusion of the component in the curricula of undergraduate education for the risks coming from the internet	2016	Administrative Cost	MEST	KCA	Curricula's are updated
2.3.8	Awareness of students through the implementation of curricula related to protection from online dangers	2016-2019	Administrative cost	MEST	MASHT, KCA, HE institutions, Inspectorate for Education	Awareness campaigns conducted
2.3.9	Preparing curricula for teaching in educational institutions regarding the protection of children online	2016-2019	Administrative Cost	MEST	MIA, KP, Relevant institutions and international partners	Curricula drafted
2.3.10	Organization of awareness raising activities about safe Internet use by children	2016-2019	Budgeted Cost	MEST	MASHT, KCA, schools, international partners	Activities organized
2.3.11	Development of an administrative instruction on the use of the	2016-2017	Budgeted Cost	MEST	KCA, parent community, international partners	Administrative Instruction approved and 12,000 manuals distributed

	Internet in schools					
2.4	**Specific objective: Legal Infrastructure**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
2.4.1	Review of the Law on Preventing and Combating Cybercrime	K1 2016	Administrative cost	MIA	Relevant Institutions and international Partners (ICITAP, ENCYSEC, OSCE, UNDP, OSCE)	Review is drafted
2.4.2	Development of Policies and Standard Operating Procedures (SOP) for computer incident response, as well as their distribution to each relevant organization facing major cyber threats;	2016-2019	Administrative Cost	National Coordinator	Relevant Institutions and international Partners (ICITAP, ENCYSEC, OSCE, UNDP, OSCE)	SOP-s are drafted
2.4.3	Drafting and adoption of the Regulation on technical requirements to guarantee security, integrity and reliability	K4 2016	Administrative Cost	RAEPC (RAECP)	Cullen International, field experts	Regulation adopted by the Board of RAEPC (RAECP)

2.4.4	The drafting and adoption of the Law on the identification and protection of critical infrastructure	K4 2016	Budgeted Cost	Ministry of Internal Affairs	Relevant Institutions and international Partners (ICITAP, ENCYSEC, OSCE, UNDP, OSCE)	Approved law in Kosovo Assembly
2.5	**Specific Objective: Human capacity building**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
2.5.1	Develop Training curriculas	2016-2019	Budgeted Cost	National Coordinator	Relevant Institutions and international Partners (ICITAP, ENCYSEC, OSCE, UNDP, OSCE)	Number of curriculas developed
2.5.2	Training and certification of personnel on Information Security	2016-2019	Donation	National Coordinator	Relevant Institutions and international Partners (ICITAP, ENCYSEC, OSCE, UNDP, OSCE)	Number of trainings and personnel certified
2.5.3	Design Scenarios and Cyber Security Exercises	2016-2019	Administrative cost	Relevant Institutions	ENCYSEC and other International Partners	The number of scenarios designed and exercises conducted
2.6	**Specific Objective: Technical infrastructure**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
2.6.1	Functionalization of the platform for the collection and registration	K2 2016	Budgeted Cost	RAEPC	MF, ENCYSEC	Platform is functionalised

	of cyber incidents (RTIR)					
2.6.2	Information technology equipment for cybersecurity	K2 2016	Budgeted Cost	RAEPC	MF	Equipment purchased
2.6.3	Advancement of equipment for Kosovo Police to investigate cybercrime	2016-2019	1,165,000 (donation)	Kosovo Police	ICITAP, international partners	Equipment purchased
Strategic Objective 3 Public and Private Partnership (PPP)						
3.1	**Specific objective: Establishment of cooperation with the private sector**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
3.1.1	Designation of focal points for cooperation with the private sector	2016	Administrative cost	National Coordinator	Private Sector	Focal points for Private Sector are designated
3.1.2	Cooperation with Internet service providers and communication for identification and protection from harmful activity	2016-2019	Administrative cost	National Coordinator	Private Sector	Number of exchanged information
3.1.3	In cooperation with the private sector, creation of the minimum	2016	Administrative cost	National Coordinator	Private Sector	Minimal mandatory defense criteria are drafted

	mandatory criteria for defense of the critical information infrastructure					
3.1.4	Organization of regular meetings between the public and private sector	2016-2019	Budgeted cost	National Coordinator	Private Sector	Number of conducted meetings
Strategic Objective 4 Incident Response						
4.1	**Specific objective: Functioning of the National CERT / CSIRT and the establishment of other CERT / CSIRT in Kosovo**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
4.1.1	Functionalization of the National CERT	K4 2016	Budgeted cost	RAEPC	ENCYSEC	Functionalization of the National CERT in RAECP
4.1.2	Establishment of the Government CERT/CSIRT at the Agency for Information Society	K2 2016	Budgeted cost	Agency for Information Society	ENCYSEC	Functionalization of the Government CERT at AIS
4.1.3	Creation of the CERT/CSIRT at MIA	K2 2016	Budgeted cost	Ministry of Internal Affairs	ENCYSEC	Functionalization of CERT-it in MIA
4.1.4	Establishment CERT/CSIRT in Kosovo Police	K2 2016	Budgeted cost	Kosovo Police	ENCYSEC	Functionalization of CERT-it in KP

4.1.5	Establishment CERT/CSIRT in MKSF	K2 2016	Budgeted cost	MKSF	ENCYSEC	Functionalization of CERT-it in MKSF
4.1.6	Establishing Web platform for reporting cyber crimes	K2 2016	Donation	Kosovo Police	ENCYSEC	Web platform established
4.2	**Specific objective: Listing and Accreditation of the CERT/CSIRT-s in Trusted Introducer and First**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
4.2.1	Formal listing of National CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	RAEPC	MIA, KP , AIS ,ENCYSEC	National CERT/CSIRT is listed
4.2.2	Accreditation of the National CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	RAEPC	MIA, KP, AIS ,ENCYSEC	National CERT is accredited
4.2.3	Formal listing of Government CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	Agency for Information Society	ENCYSEC	Government CERT/CSIRT is listed
4.2.4	Accreditation of the Government CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	Agency for Information Society	ENCYSEC	Government CERT/CSIRT is accredited
4.2.5	Formal listing of MIA CERT/CSIRT in	2016-2017	Budgeted cost	Ministry of Internal Affairs	ENCYSEC	MIA CERT/CSIRT is listed

	Trusted Introducer					
4.2.6	Accreditation of the MIA CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	Ministry of Internal Affairs	ENCYSEC	MIA CERT/CSIRT is accredited
4.2.7	Formal listing of Kosovo Police CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	Kosovo Police	ENCYSEC	KP CERT/CSIRT is listed
4.2.8	Accreditation of the KP CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	Kosovo Police	ENCYSEC	KP CERT/CSIRT is accredited
4.2.9	Formal listing of MKSF CERT/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	MKSF	ENCYSEC	MKSF CERT/CSIRT is listed
4.2.10	Accreditation of MKSF CEST/CSIRT in Trusted Introducer	2016-2017	Budgeted cost	MKSF	ENCYSEC	MKSF CERT/CSIRT is accredited
4.2.11	Membership in FIRST	2016-2017	Budgeted cost	MIA, KP, RAECP, AIS, MKSF	ENCYSEC	Membership in FIRST established
4.2.12	Participation in conferences and seminars of TI and FIRST.	2016-2019	Donation (ENCYSEC and International Partners)	MIA, KP, RAECP, AIS, MKSF	ENCYSEC, International Partners	Number of participation in conferences and seminars

Strategic Objective 5 International Cooperation						
5.1	**Specific objective: Organization and participation in international events**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
5.1.1	Organization of international cybersecurity activities and annual events	2016-2019	Donation	National Coordinator	Relevant Institutions and international Partners (ICITAP, ENCYSEC, OSCE, UNDP, OSCE)	Number of events organized
5.1.2	Participation in international activities in the field of cyber security	2016-2019	Donation	Relevant Institutions	National Coordinator, international Partners (ICITAP, ENCYSEC, OSCE, UNDP, OSCE)	Number of events and number of participants
5.2	**Specific objective: Enhancing international cooperation**					
No.	**Activity**	**Time Frame**	**Budget**	**Responsible Institution**	**Support Institutions**	**Performance Indicators**
5.2.1	Establishment of partnership with ENISA	2016-2019	Budgeted cost	National Coordinator	MIA,MKSF, KP, RAECP, AIS,	Number of visits, participation, exercises and other activities organized by ENISA
5.2.2	Advancement of regional and international cooperation in the fight against cybercrime	2016-2019	Administrative cost	KP, KIA,KC, FIU, KPC, KJC	Relevant Institutions	Number of exchanged information, number of joint investigations, number of joint operations

5.2.3	Establishment of a permanent 24/7 Contact Point for international cooperation in the field of cybercrime	2016	Budgeted Cost	National Coordinator, MIA, KP	Relevant Institutions	24/7 contact point is established