MONTENEGRO

NATIONAL CYBER SECURITY STRATEGY FOR MONTENEGRO 2013-2017

Podgorica, July 2013

CONTENTS

1. INTRODUCTION

Information and communications technology present an irreplaceable part of modern life. Integration of ICT in performing daily activities and tasks has become more and more evident, therefore, threats to information and communications infrastructure that may threaten the availability, privacy and integrity of them, may also affect the functioning of society as a whole.

The adoption of national cyber strategy is a complex task given the different aspects and stakeholders who should be included in this process. Here we can discuss about political, legislative, economic, military and similar aspects when adopting the strategy, as well as about integration of public and private sectors as infrastructure owners.

Montenegro's strategic objective is to build an integrated, functional and efficient cyberspace, in accordance with international standards and principles.

Every country is obliged to protect their national information infrastructure, as well as their cyberspace that national domain is covering.

In order to respond to cyber threats from the environment, which are constantly changing, the country must have flexible and dynamic cyber security strategies. The cross border nature of threats makes it necessary for the countries to focus on strong international cooperation. Comprehensive national cyber security strategies make the first step in this direction.

The Strategy should have clearly defined objectives and priorities, and the practice is that they are defined within a period of 5 years. Along with text of the Strategy, which presents a vision of a state against the concept of cyber security and its guaranty, the corresponding annual action plans are also defined.

Internet and information and communications technology that the Internet is based on, present a vital resource for socio-economic growth and development of a country. As more and more services have been offered via the Internet, there is a growing number of reported cyber security incidents, the attacks known as distributed denial of service attacks – DDoS attacks, up to attacks on websites with the aim of unauthorised modification of their content. Special type of threat is also an unauthorised access to developed information systems of state authorities and their databases. Cyber-attacks are also directed against infrastructure of Internet service providers (ISPs), however there is no coordinated response which would be

conducted through safe communication channels at the national level in order to address such situations.

One of the problems is the lack of necessary skills for successful defence from the incidents, as well as the need for amendments or for adopting new laws, under which it would be possible to successfully detect and prosecute people involved in any form of cybercrime.

Another important problem is that in Montenegro there is no a defined way to monitor or record the malicious traffic entering the country. There are no adequate monitoring systems installed on communication nodes (gateways) towards abroad or at ISPs level, except for detection and prevention of attacks directed towards denial of service (DoS-DDoS).

Coordinated construction of organisational, institutional and management capacities, improvement of laws and by-laws are important items of information security existence in Montenegro.

Recognising its foreign policy priorities through full membership in NATO and EU, provision of mandated safety criteria at the national level has become priority of the entire information society of Montenegro.

At the same time, economic and industrial espionage directed against the leading companies and governments is getting importance with development and progress in the field of information technology. Finally, illegal entry, data manipulation and destruction of critical resources also threaten integrity and resilience of critical infrastructure.

In cyberspace, "malicious programmes in the service of states" designate the present and in the future it will be one major threats to the national security of a country.

The above mentioned supports the fact that the Internet and related global networks have significantly increased the global dependence on ICT, but also the level of potential damage that can be caused when the infrastructure is under attack.

Information Security Strategy relies on a document adopted by the Government of Montenegro, titled ***"Study with defined responsibilities of state authorities in their fight against cyber (computer) crime"***.

Therefore, the adoption of Strategy with a clear vision in terms of implementing specific activities in the field of cyber security is crucial.

2. DEFINITIONS

The analysis of Cyber Security Strategy in great number of countries has found that there is no agreed definition of terms such as: *information security, cyberspace, cyber security, cybercrime*, etc. Whereas some strategies define these terms precisely and concisely, for example, by closely linking them to computer systems, others have a more general approach and definitions include not only matters relating to computers and computer systems, but to any other factor that may interact with them, such as human factor. In this chapter will be presented definitions of specific terms existing in our country, which are also compliant with basic meaning of the terms in EU countries.

"Cyber" is defined as: "anything relating to, or involving, computers or computer networks (such as Internet)". **Cyberspace** is more than Internet; it includes not only hardware, software and information systems, but also the people, social interaction within these networks. International Telecommunication Union (ITU) uses this term to describe "systems and services connected either directly to or indirectly to the Internet, telecommunications and computer networks". International Standardisation Organisation (ISO) uses a slightly different definition of the term, and describes "cyber" as "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". Individually, each country, when formulating national strategy, uses their own terms and definitions. For example, the United Kingdom defines cyberspace as "all forms of networked, digital activities; this includes the content of and actions conducted through digital networks".

Information security includes the state of confidentiality, integrity and availability of information. Information security is focused on data regardless of their form: electronic, printed and other forms of data.

Computer security usually seeks to ensure availability and proper functioning of the computer and computer system.

The above-mentioned terms are often alternatively used, although they are related to slightly different aspects in the field of cyber security.

Internet security in technical context, refers to "protection of Internet service and related ICT systems and networks as extension of network security in organisations and homes, and to ensure the security purpose". Internet security also provides availability and reliability of Internet service. However, in political context, Internet security is often equated with what is also known as safe use of the Internet. According to some definitions, Internet security includes a global regime dealing with stability of Internet code and hardware, as well as with agreements on prosecuting illegal content. **Network security** is also important for critical infrastructures that are often not directly connected to the Internet.

Cyber security – International Standardisation Organisation (ISO) defines cyber security as "preservation of confidentiality, integrity and availability of information in cyberspace". The Netherlands have offered a little broader definition: "freedom from danger or damage caused by disruption, failure or abuse of ICT systems" Danger or damage caused by disruption, failure or abuse may consist of a limitation in the availability or reliability of ICT systems, a breach of the confidentiality stored in them, or damage to the integrity of the information. ITU also defines broadly the cyber security: "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Cyber security seeks to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. General security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality".

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."

Cybercrime – or e-crime, or high-tech crime includes criminal activities in which computers and other IT equipment and computer network are subject, tool, target or place of crime.

Cyberspace is identified as environment with the fastest growing crime rate. Over the last decade, most countries have identified the problem of cybercrime and accordingly passed and adopted adequate laws. In 1997, China identified as illegal activity "intrusion into computer information system"; in 2004 the Council of Europe adopted Convention on Cybercrime which has relatively high standards in the field of international cooperation and for the purpose of prosecuting cybercrime, it was signed by 51 countries.

It is estimated that in 2011 appeared more than 400 million of different variations of viruses and on average 8 new "zero-day" exploits on a daily basis. This figure is an alarming fact. As the borders of legal prosecution are equal to borders of various states, strong need for close international cooperation has been identified.

Cyber terrorism – is a criminal act in cyberspace that aims to intimidate governments or their citizens, with the aim to achieve political goals. NIPC (National Infrastructure Protection Center) defines cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies".

Cyber espionage is defined as "the use of an agent in order to obtain information about plans or activities of foreign country or competitive company". It is not uncommon that companies or governments are faced with attempts of unauthorised access to their computer systems via Internet. Many countries use espionage tools to encourage their economic development based on advanced technologies of other nations. ICT present foundation of development and implementation of most other technologies both in civilian and military sectors, and thereupon they have become primary target of espionage.

Cyber war is unspecified and controversial term that has no official or generally accepted definition. More than 30 countries have accepted the doctrine and announced development of a special programme of cyber war offensive mechanisms.

3. CYBER SECURITY MANAGEMENT SYSTEM

One of key recommendations of international bodies (NATO, ENISA) is that the strategy should be developed within the life cycle, which should include the following stages:

1. Development,
2. Implementation,
3. Evaluation and
4. Adaptation strategy.

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

Public authority or internal working group or Council on the ***national*** level should be defined as strategy implementation coordinator, and should also be responsible for monitoring the overall strategy life cycle. The positive practice is that, on one hand, members of this body to be persons covering public or private function and, on the other hand, to have advanced knowledge in the field of cyber protection and security, in order to have sufficient credibility and more efficiently provide implementation of identified strategic objectives.

Successful implementation of Cyber Security Strategy requires adequate and continued cooperation of public and private sector, i.e. stakeholders from one or the other sector. The selected private entities should be part of development and implementation process because of probability that they are the owners of critical information infrastructure and service.

Development and planning of national cyber crisis plan represents an important factor in general planning of a state's cyber security. It should be realistic and accurate and it should also take into account all possible stakeholders. This includes interaction of public and private sector.

The Strategy should definitely include national risk assessment, which must be realistic, with a view to more efficient strategy implementation. During the assessment, it is necessary to have a defined methodology, as well as approach that would provide considering all possible existing threats and risks.

Important part of this process is identification and definition of critical national infrastructure, its threats and risks. These should be classified by degree of their impact, i.e. consequences that they would entail, as well as by the probability assessment of their actual occurrence.

3.1 METHOD OF MONITORING STARTEGY LIFE CYCLE

Along with constant engagement about the Strategy, which must follow the corresponding life cycle, here are indicated more specific activities that decision makers should implement:

- Define a vision, scope, objectives and priorities;
- Monitor risk assessments at the national level;
- Consider the existing policies, regulations and capacities;
- Develop clear management structure;
- Identify and engage stakeholders;
- Establish confidential information exchange mechanisms;
- Develop cyber security contingency plans;
- Organise cyber security exercises;
- Establish basic security requirements;
- Establish incident reporting mechanisms;
- Increase public awareness of this issue;
- Maintain the research and development cycle;
- Strengthen education and training programmes;
- Establish the ability to respond to incidents;
- Respond to cybercrime;
- Engage in international cooperation;
- Establish public-private partnerships;
- Balance between security and respect of privacy;
- Conduct evaluations;
- Coordinate national cyber security strategy.

3.2 CHALLENGES, RISKS, THREATS TO CYBERSPACE SECURITY IN MONTENEGRO

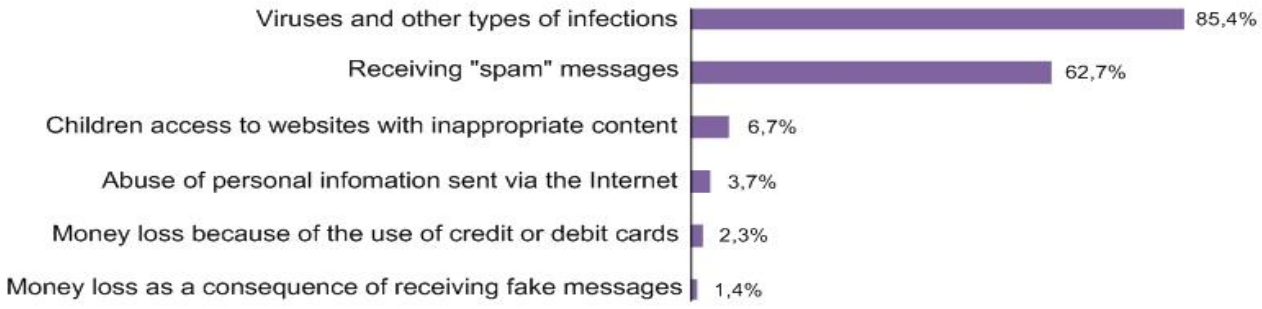
Research on the use of information and communications technology in Montenegro, conducted by the Statistical Office of Montenegro in 2012, provided the following results:

Households:

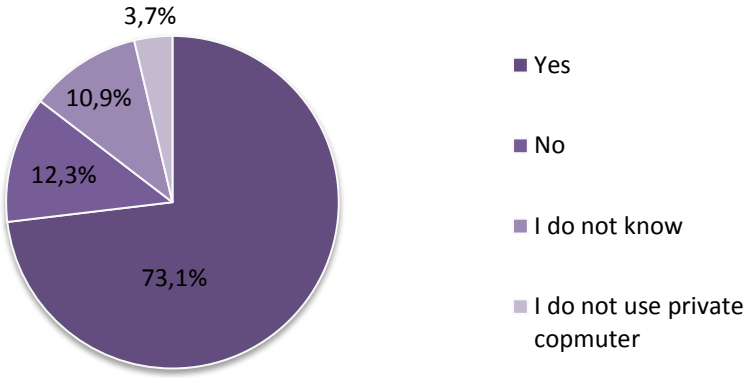
- 51.3% have access to personal computer (PC),
- 33.6% of households use laptop
- 93.3% have a mobile phone.

In Montenegro, 55.0% of households surveyed said they had Internet access at home. Internet access is thereby achieved by means of a certain device such as personal computer (PC) – 75.3% of households and laptop – 52.0%. In addition to these devices, to access the Internet they also use mobile phones – 24.2%, handheld computers (palmtop, PDA, tablet), game consoles (Play Station), etc.

To the question "Have you in the last 12 months encountered any of the problems related to security while using the Internet for private purposes?", citizens responded as follows:



To the question whether they use IT security software to protect their private computer and data kept in it (antivirus, anti-spam, firewall, etc.), the following results have been obtained:



Business entities:

In Montenegro, 88.3% of companies surveyed stated that they used computers in their operations during January 2012.

According to survey results, 53.3% of the companies (who used computers in their operations) allowed their employees a remote access to e-mail system, documents or company applications in January 2012.

As regards to the Internet, the survey showed that 96.1% of companies who used the computer, had access to the Internet in January 2012. This represents an increase of 1% in comparison to the previous year. Out of the companies that had access to the Internet, 53.1% responded that they had a Web Site/Home Page, in January 2012.

To the question about the employing IT professionals in January 2012, only 20.8% of companies responded that they employed professionals whose main job is information technology.

In Montenegro, only 27.9% of companies have the Rulebook that normatively regulates information security issues. There is also a very small percentage of companies that conduct assessment of employees knowledge about information security measures, only 26.9%.

Key risks, challenges and threats to cyber security in Montenegro include the following:

a. Shortcomings in organization of cyber protection may pose a threat to national security of Montenegro;

b. Internet in Europe and in our close environment is intensively used for criminal purposes, for the purposes of drug trafficking, money laundering and financial frauds, thereupon Montenegro is not and will not be spared from this threat;

c. ICT infrastructure, computer systems and users in Montenegro are exposed to most of cyber threats and attacks that affect the rest of the world. This includes malicious programmes, electronic frauds, web page headline changes (Web Defacement) and e-mail "hacking";

d. Undeveloped cooperation between private and public sector in the field of coordination of critical infrastructure security system;

e. The absence of procedure about keeping records on incident situations in cyberspace of Montenegro;

f. The absence of National Cyber Security Council with its functions:

    i. Coordination of information security in Europe

    ii. Identification of critical information infrastructure

    iii. Review of the legislative framework for the development of operational cyber security.

g. Cyberspace is increasingly used for organisation and media propaganda of extremist and radical groups who by this way promote their activities, recruit new members, organize terrorist actions, and thus pose a threat to national security of Montenegro.

h. Piracy contributes to high rate of infection with computer viruses.

i. On-line manipulations, using social engineering by means of e-mail messages, such as *"Nigerian 419"* scam, *phishing*, go hand in hand with identity theft (illegal knowledge of other users' accounts and passwords). This situation in Montenegrin cyberspace is worrying and problematic, not only for Montenegro, but even wider. Montenegrin citizens have in the past been the target of frauds in which they even happened to lose a great sum of money;

j. In the period from 2008 to 2013, the attackers have changed or taken control over several websites of Montenegrin institutions;

k. In Montenegro, in the past period there have been several attacks on information infrastructure, Internet service providers as well as on the banking sector;

l. In previous years there has been observed a significant number of cases where the attackers took control over the user profiles of Montenegrin citizens on social networks and on behalf of the user entered inappropriate content, in order to compromise the profile owner.

m. From the addresses, for which it has been investigated to come from Montenegro, malicious activity has been reported, including the spread of SPAM, password-cracking attacks by using force (brute force), DDoS attacks, impersonation, and others;

n. In Montenegro, there is a very small number of staff who have highly specialized knowledge in the field of cyber security, i.e. who have certain licenses or certificates from this field required by European and international standards. At the University of Montenegro, there are no faculties or faculty departments that cover cyber security and forensics, i.e. which produce human resources with highly specialized knowledge in this field.

4. INSTITUTIONAL AND LEGISLATIVE FRAMEWORK OF MONTENEGRO

4.1. Analysis of Montenegrin and EU legislation

Over the last couple of years, Montenegro has begun, through the criminal law reforms, to build a corresponding legal and regulatory framework that legally prevents any kind of accidental or deliberate distortion and prevention of the computer system functioning. An appropriate legal framework represents a link between legal and IT areas, which will, by joint cooperation, contribute to successful clarification of the case in the field of computer crime and punishing the perpetrators.

In Dubrovnik, on 15th February 2013, Montenegro signed regional Declaration on Strategic Priorities against Cybercrime, which identifies strategic priorities in the fight against cybercrime that this Strategy follows and continues to evolve.

European Convention from 1959 on the provision of mutual legal assistance in criminal matters represents a predecessor of the Convention on Cybercrime, which has been adopted to serve as a framework to the states wishing to legally codify this kind of socially dangerous behaviour.

The Convention on Cybercrime or known in the international community as the Budapest Convention, was adopted on 21st November 2001 by the Council of Europe, and is effective from July 2004.

The Convention was signed by 51 countries, from which six countries are not members of the Council of Europe and these are Australia, the Dominican Republic, Canada, Japan, South Africa and the USA.

This Convention is one of framework conventions, which means that its provisions are not directly applicable, but it is necessary that states implement these provisions in their own, i.e. national legislation.

Montenegro adopted the Law on Ratification of the Convention on Cybercrime on 3rd March 2010, which entered into force on 1st July 2010. In addition, Montenegro also ratified the Additional Protocol on Xenophobia and Racism (CETS 189) along with the Convention from

3rd March 2010, which entered into force on 1st July 2010. Montenegro has signed and ratified the Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201).

Criminal offenses indicated under this Convention as cybercrime include a wide range of spreading viruses, unauthorized access to a computer network through piracy to pornography and intrusion into the banking systems, abuse of credit cards and all other criminal offences in which computers are used. Montenegrin criminal legislation complies with the provisions of Budapest Convention.

Budapest convention stipulates that national legislations in their criminal codes are to provide punishment for offenses related to infringement of copyright and related rights, and liabilities assumed by the Bern Convention for the Protection of Literary and Artistic Works, protection by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and World Intellectual Property Organization (WIPO) Copyright Treaty. Codification of these criminal offenses in our Criminal Code has been provided in provisions related to violation of moral rights of authors and performers, unauthorized use of copyright works and objects, unauthorized circumvention of protection measures intended to prevent violations of copyright and related rights, unauthorized removal or alteration of electronic information on copyright and related right, unauthorized use of other's patent, unauthorized use of other's design.

The Convention also includes liability of legal entities, and when it is translated into our national legislation, then we can say that in 2007 Montenegro adopted the Law on liability of legal persons for criminal offenses. Article 3 of this Law stipulates that legal entities can be held accountable for all the criminal offences from the special section of the Criminal Code, as well as for all other criminal offenses prescribed by a special law, provided that the conditions for liability of legal entities prescribed by the Law on liability of legal entities for criminal offenses have been met.

Montenegro ratified the Additional Protocol to the Convention on Cybercrime and the **Protocol involves punishment for acts of racism and xenophobia, which are made by computer systems.** This Protocol was ratified on 3rd March 2010 and entered into force on 1st July 2010. The Protocol is implemented as a separate article of the Criminal Code, which involves instigation of national, racial and religious hatred.

EU Council Framework Decision 2005/222/PUP or EURLex number 32005F0222 includes attacks on information systems, and it has been implemented through the provisions of Criminal Code.

In addition, a very important international source of law is the **EU Council Framework Decision 32000D0375**, which was adopted on 29th May 2000. It includes combating child pornography on the Internet and provides a number of specific measures on the aim to prevent and combat production, processing, possession and distribution of child pornography material and on the aim of efficiency of investigation and of criminal prosecution of offenses from this field. Criminal Procedure Code of Montenegro provides measures for which we can say to partially comply with this Framework Decision, and it is about the urgency of the proceedings when these works are concerned, exclusion of public for these offenses, provided that these are general provisions concerning procedures relating to minors.

Procedural Law

The Convention on Cybercrime also involves procedural provisions for the field of cybercrime. The Convention recommends to States Parties to adopt all appropriate legislative and other measures in their national legislatures in order to establish certain powers and procedures for the punishment of criminal offenses related to cybercrime.

Montenegro adopted a new Criminal Procedure Code, which is in accordance with international legal standards and fully or partially complied national procedural norms with certain procedural provisions stipulated by Budapest Convention. Equally, Convention Articles relating to evidentiary actions, secret surveillance measures and temporary seizure of objects and confiscation measures have been implemented in our criminal Procedure Code.

Legislative framework

Legal documents that form the basis of the functioning and further development of modern concept of information security in Montenegro:

a) Law on Ratification of the Convention on Cybercrime

b) Criminal Code

c) Criminal Procedure Code

d) Law on Information Security

e) Law on the National Security Agency

f) Law on Classified Information

g) Electronic Signature Law

h) Law on Electronic Communications

i) Electronic Commerce Law

Other important documents that need to be mentioned in this chapter:

- Study with defined responsibilities of state authorities in fight against cybercrime including assessment of the state condition and readiness in the area of cyber security
- Regulation on detailed conditions and method of implementing IT measures to protect classified information (1st July 2010)
- Regulation on detailed conditions and method of implementing measures to protect classified information (6th November 2010)
- Regulation on detailed conditions and method of implementing industrial measures to protect classified information (16th December 2010)
- Regulation on method of conducting and content of internal control over implementation of measures to protect classified information (28th July 2010).

4.2. Accountable institutions for Montenegrin Cyber Security System

Within public administration, there must be a defined organizational hierarchy that will most efficiently and in a long-term sustainable manner ensure the appropriate security information management in Montenegro.

The following institutions have been identified as crucial in the field of cyber security in Montenegro:

- Ministry for Information Society and Telecommunications (National CIRT)
- Ministry of Defence
- Ministry of the Interior
- Ministry of Justice
- National Security Agency
- Police Administration
- Military of Montenegro
- Directorate for the Protection of Classified Information
- Universities of Montenegro

National CIRT is a central point for coordination and exchange of information, cyber defense and elimination of the consequences of cyber security incidents for the area of Montenegro.

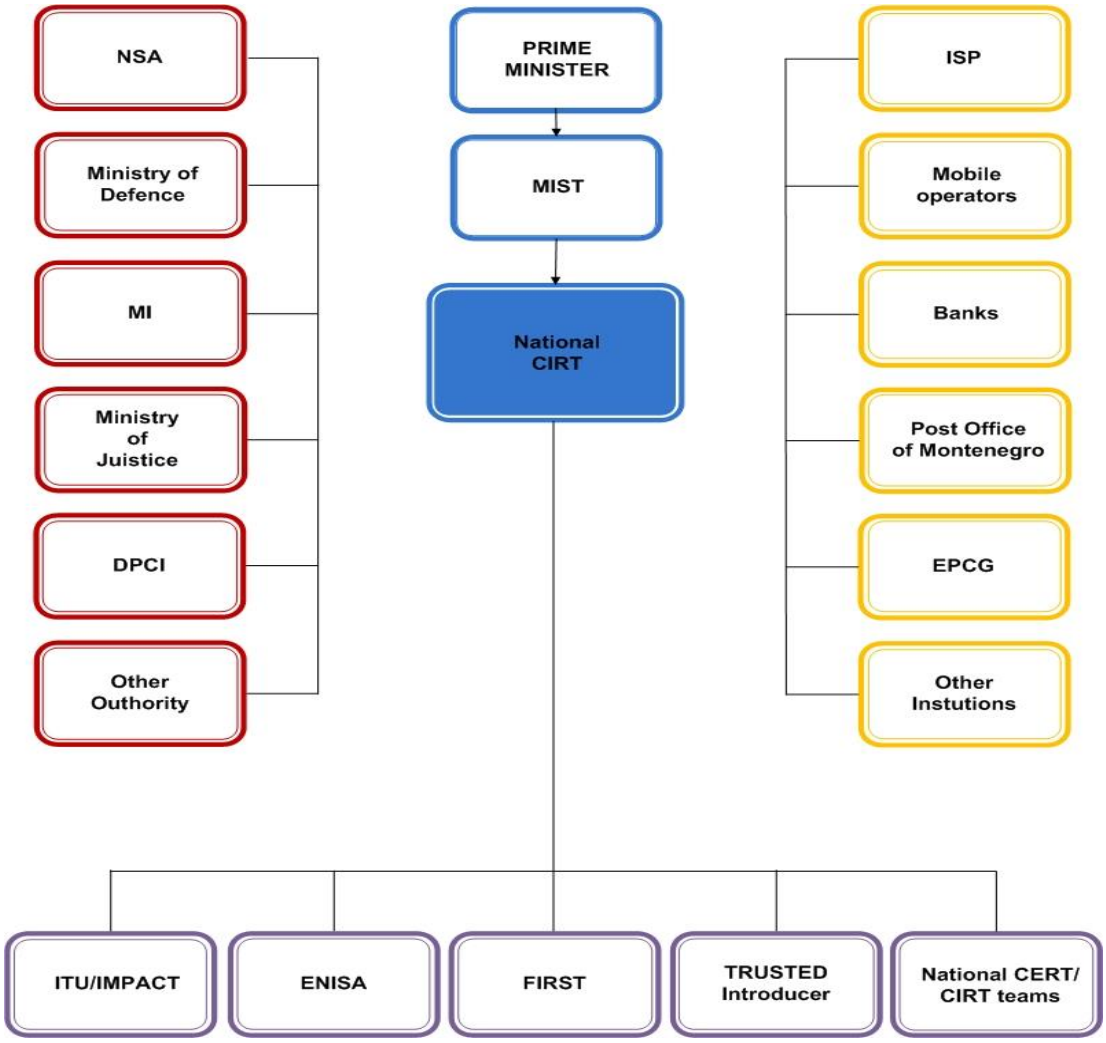


Figure 1: Position of National CIRT in Cyber Security System of Montenegro

Members of this hierarchical infrastructure are also CIRTs or similar organizational bodies established by Internet Service Providers (ISPs), mobile operators, banks, Post Office of Montenegro, EPCG and other companies that are interested or have significant impact on the functioning of national information infrastructure.

CIRT has become a member of key international institutions that are relevant in the area of cyber security, such as FIRST (Forum of Incident Response Security Teams); TRUSTED Introducer (TERENA), ITU-IMPACT coalition. Membership in this organization provides for CIRT to connect with other CERT/CIRT teams from around the world.

5. MAIN OBJECTIVES OF CYBER SECURITY STRATEGY FOR MONTENEGRO

Cyber Security Strategy for Montenegro contains seven key areas:

1) Defining institutional and organisational structure in the field of cyber security in the country

Coordinated construction of organizational, institutional and management capacities, improving laws and regulations are important items of information security existence in Montenegro.

The formation of National Cyber Security Council means providing umbrella organisation in the country that will advise the Government of Montenegro on all important matters related to cybercrime. The Council will propose measures for harmonisation of legislative and administrative framework with a view to more efficiently fight against cybercrime.

Council members are representatives of key institutions identified in the fight against cybercrime.

Key activities:

- Establishment of National Cyber Security Council
- Establishment of local CIRT teams

2) Protection of critical information structures in Montenegro

Due to constant grow of the number of services that state authorities and private sector provide to citizens as well as to other legal entities, it is necessary to define a critical information infrastructure in Montenegro and develop protection procedures.

It is necessary to provide national cyber security and protect economic interests. Therefore, the Government needs to provide necessary structure and resources to ensure cyber security.

Key activities:

- Definition and protection of critical information infrastructure
- Strengthening the resilience of information systems to incidents
- Perform analysis of threats to IT infrastructure

3) Strengthening capacities of state law enforcement authorities

Constant improvement of the sophistication level of cyber threats and attacks, as well as their methods and technics require continuous strengthening of administrative capacities of a state for the purpose of responding efficiently to a wide range of cyber threats.

Computer crime (cybercrime) and electronic evidence material require 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.

Key activities:

- Adopting full and effective legal solutions in the field of cybercrime, which meet the requirements of human rights and the rule of law
- Strengthening of specialised unit for fight against cybercrime within the Police Administration
- Strengthening of specialised unit for fight against cybercrime within the Military of Montenegro
- Strengthening the capacity of National Security Agency in the field of collecting, recording, analysing, storing and exchanging data from cyberspace, and in accordance with the Law on National Security Agency
- Improving capacities for digital forensics

- Strengthening the capacity of prosecution in the area of cybercrime and electronic evidence material
- Support the training of judges, prosecutors and law enforcement authorities in the field of computer crime
- Promoting financial investigations and preventing fraud and money laundering on the Internet

4) Incident Response

By establishing the National CIRT at the Ministry for Information Society and Telecommunications, a big step has been taken towards preventing and eliminating cyber threats that affect the state and its citizens. In cooperation with key institutions in Montenegro, CIRT is dealing with detection, monitoring and prevention of cyber attacks and cybercrime at the state level. CIRT represents a central point for coordinating prevention and protection against computer security incidents on the Internet and other IT security risk for the area of Montenegro. It is also possible to report incidents on the website www.cirt.me.

In order to respond to incident situations in the best and most efficient possible manner, it is necessary to ensure better cooperation and free information exchange between key institutions in the field of cyber security. This primarily relates to cooperation of key state institutions with key institutions from private sector (Internet Service Providers, agent for .me domain, mobile operators, banking sector, electric power, post office, etc.).

Also, given that cyber attacks are unlimited and that a large number of cyber attacks come from other countries, it is necessary to establish and maintain cooperation with relevant international institutions (FIRST, Trusted Introducer, ITU-IMPACT, etc.) and national CERT/CIRT teams from other countries.

Key activities:

- Provide through National Cyber Security Council the procedure for information exchange between state authorities and administration bodies
- Provide trainings for employees who work in the field of cyber security within CIRT
- Enhance cooperation with key institutions from private sector
- Continue with activities on cooperation of national CIRT of Montenegro with key international organisations and CERT/CIRT teams from other countries.

5) The role of Ministry of Defence and Military of Montenegro in cyberspace

Given the increasing role of information technology in military operations, and the need to protect against malicious cyber activities, it is necessary to consider the role of the Ministry of Defence and the Military of Montenegro in protecting cyberspace of Montenegro. The impact of cyber security in military domain varies from country to country, as the definition of military cyber operations also varies.

According to some NATO reports, about 120 countries develop military cyber capacities.

Key activities:

- Define the role of the Ministry of Defence and Military of Montenegro in cyberspace of Montenegro
- Strengthen the capacity of Ministry of Defence and Military of Montenegro in the field of cyber defence
- Establish cooperation in this field with international partners.

6) Public-private partnership

Major part of critical information infrastructure belongs to the private sector. Therefore, 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 providers
- Agent for .me domain
- Banking sector
- Electric Power
- Companies that host e-services in Montenegro

7) Raising public awareness and protection on the Internet

Ensuring safer Internet environment for citizens of Montenegro and training of users through raising awareness of the need for training need to be done. Special focus should be on 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.

Key activities:

- Organise projects and campaigns to promote safe use of the Internet with special focus on child protection on the Internet
- In cooperation with the Ministry of Education and universities in Montenegro, work on organizing special programs from the area of cyber security with the aim of creating staff with highly specialized knowledge from this field
- Efficient regional and international cooperation.

ANNEX I: ACTION PLAN FOR STRATEGY IMPLEMENTATION 2013-2015

NO.	TASK	DESCRIPTION	RESPONSIBLE AUTHORITY	DEADLINE
1	Establish National Cyber Security Council (information security)	Council members are representatives of institutions that are identified as key in the field of cyber security. Government of Montenegro will appoint Council members upon recommendation of the Ministry for Information Society and Telecommunications (MIST). Responsibility of the Council will be activities from the domain of cyber security and INFOSEC.	MIST	December 2013
2	Establish local CIRT teams in key institutions to fight against cyber crime with a view to establish National CIRT infrastructure	All state authorities and administration bodies who maintain a database of national importance or manage critical part of IT infrastructure need to form local CIRT teams.	MIST	March 2014
3	Definition and protection of critical information infrastructure	Define Methodology to be used for the purpose of identifying critical information infrastructure. It is necessary to define critical information infrastructure in Montenegro and develop procedures for protection to ensure its smooth operation.	MIST MD MI NCA	September 2014
4	Improve cooperation between state authorities and administration bodies	Provide through the National Cyber Security Council the procedure for information exchange between state authorities and administration bodies		May 2014

5	Provide trainings for employees who work in the field of cyber security within national CIRT and local CIRT teams	In order to respond to incidents in the best and most efficient possible manner, it is necessary to provide vocational training of staff who work on resolving the incidents.	MIST	January – December 2014
6	Improve cooperation between public and private sector	Provide through National Cyber Security Council the procedure for information exchange between state authorities and key institutions from private sector, in particular: • Internet providers • Agent for .me domain • Banking sector • Electric power • Companies that host e-services in Montenegro Depending on conducted Analysis, the Council will define the manner of cooperation with other entities.	MIST MD MI NCA	July 2014
7	Conduct cyber threat analysis in Montenegrin cyberspace	Due to constant grow of the number of services public and private sector provide to citizens as well as to other legal entities, we must strive to protect cyberspace of Montenegro. The first step is analysis of cyber threats.	MIST MD MI NCA	December 2014
8	Organise projects and campaigns to promote safe use of the Internet with special focus on child protection on the Internet	Ensure safer Internet environment for citizens of Montenegro and training of users through raising awareness of safe use of the Internet. Special attention to be paid to campaigns and promotion of child protection on the Internet.	MIST	March 2014

9	Strengthen the specialised unit for fight against cybercrime within the Police Administration	In order to ensure smooth prosecution of offences against computer data and systems, offences committed over computers, it is necessary to improve capacities of specialised unit for fight against cybercrime within the Police Administration	MI	By the end of 2014
10	Improve capacities for digital forensics	It is necessary to improve capacities of the Forensic Centre in Danilovgrad to ensure adequate collection and analysis of electronic evidence material.	MI	September 2015
11	Strengthen capacities of the Ministry of Defence and Military of Montenegro in the field of cyber defence	Define the role of Ministry of Defence and Military of Montenegro in cyberspace of Montenegro	MD, Military of Montenegro	March 2015
12	Organise conferences/trainings on cyber security	Provide the basis for organising regional conference/training on cyber security on an annual basis. This provides for improvement of regional cooperation, raise of awareness and promotion of Montenegro as one of the leading countries in the region in this field.	MIST MD MI	October 2015