Deliverable 1.3

Cross-matching of practice in ME with EU standards

Tempus

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

Deliverable 1.3

Cross-matching of practice in ME with EU standards

European Commission Tempus Project:

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of content

1. Introduction and preliminaries

Every state has to protect their own national IT infrastructure, as well as cyber space which is covered by the national domain.

The strategic goal of Montenegro is to develop an integrated, functional and efficient cyber space, in accordance with international standards and principles. In order to efficiently respond to cyber threats in a constantly changing environment, countries have to have more flexible and dynamic strategies concerning cyber security. The key document that has been adopted by the Government on September 12th 2013 is the »The Strategy in Cyber Security of Montenegro from 2013 to 2017« with the proposed action plan for implementation of the strategy from 2013 to 2015.

The strategy of IT security is based on a document adopted by the Government of Montenegro in 2012. It was named »Study with defined responsibilities of state authorities in their fight against cyber (computer) crime«.

The main goals of the strategy in Montenegro's cyber security

Cyber Security Strategy for Montenegro contains seven key areas:

1. Defining institutional and organisational structures in the field of cyber security in the country
2. Protection of critical information structures in Montenegro
3. Strengthening capacities of state law enforcement authorities
4. Incident Response
5. The role of Ministry of Defence and Military of Montenegro in cyberspace
6. Public-private partnership
7. Raising public awareness and the protection on the Internet

To achieve the main goals, an action plan has been adopted for the implementation of the strategy from 2013 to 2015.

According to the strategy, the key risks, challenges and threats to cyber security in Montenegro are:

1. Negligence of cyber protection may pose a threat to the national security of Montenegro
2. Internet in Europe and in our close environment is intensively used for criminal purposes, for the enabling drug trafficking, money laundering and financial frauds, thereupon Montenegro is not and will not be spared from this threat;
3. The ICT infrastructure, computer systems and their users in Montenegro are exposed to the majority of cyber threats and attacks like the rest of the world. This includes malicious programmes, electronic frauds, web page headline changes and e-mail »hacking«;
4. Undeveloped cooperation between the private and public sectors in the field of coordination of security of critical infrastructure systems,

5. The absence of procedure about keeping records on incident situation in Montenegro's cyber space;
6. The lack of a National Cyber Security Council with its functions:
   a. The coordination of information security in Montenegro
   b. Identification of critical information infrastructure
   c. Review of the legislative framework for the development of operational cyber security.

2. Relevant Organizations and Institutions

2.1 National Organizations in Montenegro

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.

In Montenegro, the key institutions essential to the field of cyber security are:

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

Ministry of the Interior

The main goal of the Ministry of the Interior in the field of cyber security is to enforce specialised units so they can fight off any kind of cyber criminality within the Police Directorate, to enable the smooth processing of offenses against computer data and systems as well as illegal acts that can be done with the help of a computer. It is also important to enhance the capacity of the Forensic centre in Danilovgrad in order to enable proper gathering and analysis of digital evidence material, that is, procedures in the area of digital forensics.

Ministry of Defence

Having in mind that ICT has a big role in military operations and our need to protect ourselves from all kinds of threats, we need to develop installations connected to the military to protect the cyber space of Montenegro. All modern military installations are connected to cyber space. For instance, according to some NATO reports, about 120 countries are developing military connected cyber installations.

Considering that the strategic goal of Montenegro, are Euro-Atlantic integrations, the policy for cyber security, Montenegro adapts to corresponding NATO standards.

The key activities are: defining the role of the military in the cyberspace of Montenegro, strengthening the capacity of the Military of Montenegro in the field of cyber defence and the establishment of cooperation in this field with international partners.

Strengthening the capacity of national law enforcement authorities

Constant improvement of the level of sophistication of cyber threats and attacks, as well as their methods and techniques requires continuous strengthening of the law enforcement capacity of a country in order to respond effectively to a wide range of cyber threats.

Computer crime (cybercrime) and digital evidence material require a specialized response of the criminal justice authorities. Law enforcement authorities and prosecutors should be able to conduct investigations and prosecute offenses against computer data and systems, offenses committed with the help of computers and electronic evidence related to any offense.

Key activities:

- Adoption of complete and effective legal solutions in the field of cybercrime, which meet the requirements in the field of human rights and the rule of law.
- Strengthening of specialized units to combat computer crime within the Police Directorate.
- Strengthening of specialized units to combat computer crime within the Military of Montenegro.
- Strengthening the capacity of the National Security Agency in the areas of collecting, recording, analysing, storing and exchanging data in cyberspace. It should be in accordance with the law of the National Security Agency.
- Improve the capacity of digital forensics

Universities of Montenegro

In educational institutions, special focus should be given to the new generations, as well as end-users of the Internet and we should continuously introduce new programs about information security at all educational levels in order to use advanced information systems. It is also necessary to provide a safer internet environment for the citizens of Montenegro and to educate users by raising their awareness of the need for further education. Universities in Montenegro, as agents of the process of higher education, need to work on organizing special programs in the field of cyber security, with the aim of creating a staff with specific knowledge in this area.

Ministry for Information Society and Telecommunications (National CIRT)

The national CIRT represents a central place for coordination and exchange of data, defence from cyber-attacks and the elimination of the consequences of cyber security incidents for Montenegro.

Montenegrin CIRT was established in accordance with the Law on Information Security of Montenegro, within the Ministry for Information Society and Telecommunications (MIST) formed as a separate organizational unit of the Ministry, which operates within the Department of IT infrastructure and will cover the area of the national CIRT. CIRT is engaged in the handling of information security incidents, if one party involved in incident is in Montenegro (if it belongs to ».me« domain or if it is within Montenegrin IP address space).

Mission statement

- CIRT.ME shall coordinate and assist government agencies in implementing proactive services to reduce the risks of computer security incidents as well as respond to such incidents when they occur.
- CIRT.ME shall conduct awareness campaigns in order to educate the local population about the adverse effects of cyber threats and cybercrime.
- CIRT.ME shall handle safety warnings and advise its users (e.g. people, government employee, etc.).

As a part of its operations CIRT is implementing proactive and reactive measures. Proactive measures act before the incident and other events that could endanger the security of information systems occurs, in order to prevent or mitigate potential damage. Reactive measures present assistance in identifying the perpetrators and restore system in the working condition.

CIRT activities are:

- Coordination and communication:
  - Coordination of activities of local CIRT teams in Montenegro
  - Maintaining contact with other state bodies, legal entities and individuals in terms of preserving and improving information security
  - Exchange of information with national CIRT teams of other countries through membership in international organizations
- Prevention, treatment and elimination of consequences of computer security incidents on the Internet and other information systems security risks:
  - Prevention is reflected in the proactive mode of action, which involves providing information and assessment of information security, vulnerability testing, collecting, recording and processing data on incidents, testing and implementation of new software and hardware systems for the protection of IT resources
  - Data processing and elimination of consequences consists in: determining the occurrence and severity of the incident, the cause of the incident, the mediation in communication between all parties involved in the incident, the reporting of other CERT / CIRT / CSIRT teams, preparation of reports and warnings to other users, eliminating vulnerabilities in the system, protecting systems against possible incidents, forensic analysis
- User education in the field of information security includes:
  - Setting publications, manuals, software tools and other useful information relating to safer use of information technology on the web portal (www.cirt.me)
  - Organizing courses and training on topics of: IT security and the possible means of protection and prevention of computer-security incidents

The main service CIRT provides to its users is – incident handling, response and coordination. The Security Advisors at CIRT.ME will respond to telephone calls and e/mails from users and mediate the communication between applicants and the corresponding addresses that are in connection with the attacks and include third parties. CIRT.ME is a trustworthy mediator between users who have to contact foreign internet providers, foreign CIRT's, Governments and other bodies related to IT and computer safety.

Resources

International Telecommunication Union (ITU) founded in 1865, it has 193 member states and has a leading role in the field of ICT technologies, on an international level.

International Multilateral Partnership against Cyber Threats, IMPACT, based in Malaysia, it is the operational home of ITU's Global Cyber security Agenda (GCA). It has 192 member states to whom they provide their expertise and resources in order to effectively deal with cyber threats.

2.2 Experience in cyber security field

By establishing a national CIRT at the Ministry for Information Society and Telecommunications, we made a big step towards preventing and eliminating cyber threats that could potentially affect the state and its citizens. The CIRT alongside with key institutions in Montenegro deals with the detection, monitoring and the suppression of cyber-attacks and cybercrime at state level.

In order to respond to incidents in the most efficient way, CIRT has a good cooperation and information exchange between key institutions in the field of cyber security. This primarily refers to the cooperation of state institutions with key institutions in the private sector (Internet Service Providers, agent for the ».me« domain, mobile operators, banking sector, the power distribution company, post office, etc...).

Incident report is also possible on the official web portal www.cirt.me.

Below is a statistical overview of reports related to cyber security for the last year:

- State authority reports -19
- Reports made by commercial banks - 3
- Reports made by foreign partners - 6
- Reports from legal entities in Montenegro - 3
- Reports made by individuals - 27

3. Cyber security standards and frameworks

3.1 Legal framework for cyber security in Montenegro

Since 2005, Montenegro has started creating its institutional and legal framework, which prevents any kind of accidental or intentional breach or incapacitating of informational system, through reform of its criminal legislation.[1] Adoption of new and improvement of existing primary and secondary legislation, represents key element for existence of information security in Montenegro. Adequate legal framework represents a link between areas of law on the one side, and information technology on the other side, which should contribute to successful resolving of cases in the field of cyber-crime, and to sanctioning of perpetrators.

Key legal acts, which constitute the base for functioning and further development of contemporary concept of information security in Montenegro, are:

1. Law on Ratification of Convention on Cybercrime;
2. Criminal Code;
3. Code of Criminal Procedure;
4. Law on Information Security;
5. Law on Agency for National Security;
6. Information Secrecy Act;
7. Law on Electronic Signature;
8. Law on Electronic Communications;
9. Law on Electronic Trade;
10. Cyber Security Strategy in Montenegro 2013-2017;
11. 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
12. Regulation on detailed conditions and method of implementing IT measures to protect classified information (1st July 2010)
13. Regulation on detailed conditions and method of implementing measures to protect classified information (6th November 2010)
14. Regulation on detailed conditions and method of implementing industrial measures to protect classified information (16th December 2010)

[1] Montenegro has ratified Budapest Convention on Cybercrime in 2005, followed by adoption of the Law on Ratification of Convention on Cybercrime on 03/03/2010, which entered into force on 01/07/2010. Montenegro has also ratified additional Protocol on Racism and Xenophobia, as well as Convention on protection of Children from Sexual Exploitation and Sexual Abuse. At the same time, Montenegro constantly aligns its legislative with provisions of Framework decision of CoE 32000D0375. Montenegro is signatory to the Regional Declaration on strategic Priorities in Fight against Cybercrime (Dubrovnik, 2013).

15. Regulation on method of conducting and content of internal control over implementation of measures to protect classified information (28th July 2010).

Due to necessity to explain the most important documents, which create legal framework for the fight against cybercrime, in further text we offer analysis of few key legal documents in this area.

Within the framework of ***Criminal Code***, Montenegro has introduced chapter »Criminal Acts against Safety of Computer Data«, encompassing all criminal acts of high-tech crime. This, XXVIII Chapter of Criminal Code, defines following criminal acts: *criminal act against security of computer data, unauthorized access to computer system*, *disturbing of computer system, abuse of devices and programs, creation and transmission of computer viruses and computer fraud.* Taking over key terms and definitions from international documents, Montenegro aligns its national legislation with international and European standards in this area.

Article 353 of Criminal Code defines criminal act *unauthorized access to computer system*, which comprises »unauthorized access to computer system, either as a whole, or any part of it, and it manifests in basic form or in two more grave forms« and it contains five elements of this criminal act.[2] Paragraph 1 of Article 353 defines basic form of this criminal act and sets financial sanction or up to one year of imprisonment. If more grave forms of this criminal act are committed (paragraphs 2, 3 or 4, i.e. in cases of unauthorized access to protected computer, computer network, unauthorized interception of computer data or destroying of such data, while more grave forms of this act include breach of security system of protection, i.e. breach or access to specific computer through violation of security mechanisms) Criminal Code determines financial sanctioning or sanction of imprisonment in duration of three to five years.

Criminal act of unauthorized use of computer, without knowledge of computer user/owner, can be committed by any individual. These persons are recognized by the law as »hackers«. They have different motives for illegal access to computer systems, and they are trained to overcome even the most complicated protective measures that computer can have. Special form of this criminal act exists in case of unauthorized interception of computer data. This doesn't include any interception of data, but only those data that can't be publicized. Sanctions foreseen for this criminal act are financial penalty and imprisonment for up to three years.

Article 350 of Criminal Code defines criminal act »*disturbing of computer system*«[3] which encompasses illegal and higher-degree disturbing of computer systems, done by entering, destroying, deleting, altering, damaging or concealing of computer data. For perpetrators of basic form of this violation, Criminal Code foresees financial penalty or sanction of imprisonment in duration of 3 years, while in cases of graver form of this act (when act is committed on the system which has public significance, or significance for state bodies public services and commercial societies) Criminal Code foresees sanction of imprisonment for 1 to 8 years.

---

[2] In earlier versions of Criminal Code, criminal acts »unauthorized access to protected computer and computer network« and »prevention and limitation of access to computer network« were special criminal acts, while now they are paragraphs of more general »unauthorized access to computer system« criminal act, defined by Article 353 of CC.

[3] This criminal act was previously defined under term »computer sabotage«.

Article 354 of Criminal Code defines criminal act »abuse of devices and programs« and it incriminates production, sale, procurement for use and placing on disposal of any device, or instrument, which can be used to perform all criminal acts from Chapter XVIII of Criminal Code, i.e. for performing of all criminal acts in relation to computers. For this criminal act, a sanction of imprisonment in duration on 3 months up to 3 years is foreseen.

Article 351 of Criminal Code defines criminal act »production and entering of computer viruses«. In case of entering of virus into computer system, law foresees financial penalty or sanction of imprisonment in duration up to one year, and if entered virus has produced any damage, heavier financial penalty and imprisonment up to two years are foreseen. Article 142 of Criminal Code defines the term »computer virus«: program which endangers or alters functions of computer system, i.e. program which endangers or uses computer data without permission«.

Article 352 of Criminal Code defines criminal act »computer fraud« which takes central place in group of computer criminal acts. Computer fraud is defined as »any alteration, erasing or concealing of computer data, or any disturbance of work of computer system, which affects result of electronic processing, data transmission and functioning of computer system, having fraudulent intentions, i.e. with intention to obtain unlawful property gain for him/herself or for another and thereby causes property damage to another«. For perpetrators of this act in basic form, a sanction of imprisonment in term of 6 months to 5 years is foreseen. For graver forms, which exist if property gain obtained, or damage created has surpassed the limit of 3000€, sanction foreseen is at least 2 years up to 10 years in prison, whereas if the gain/damage limit has surpassed 30.000€, sanction reaches from 2 up to 12 years in prison. This criminal act is considered specialized criminal act under general criminal act of fraud, as it really is a special form of fraud. What differentiates this act from classic act of fraud is lack of elements of »bringing a person to delusion or keeping it in delusion«, because it is essentially impossible to do, so computer fraud can't be classified under general act of fraud.

Besides mentioned criminal acts, situated in special Chapter of Criminal Acts against Safety of Computer Data of Criminal Code, by Article 211 of Criminal Code is incriminated act defined as »*displaying of pornographic material to children, production and possession of child pornography*«.

Criminal code foresees sanctions for acts related to violation of copyrights and similar rights. Taking in consideration that most of these acts is done through computer system, they can be brought under broader concept »cybercrime«. These criminal acts are defined by Articles 233-238 of Criminal Code, which list following criminal acts:

- Violation of moral rights of authors and performers;
- Unauthorized use of copyrighted work or objects;
- Unauthorized circumvention of the protection measures intended to prevent violation of copyright and related rights;
- Unlawful removal or modification of electronic information on copyright and related rights;
- Unlawful use of someone else's patent and unauthorized use of someone else's design.

Additionally, Articles 260, 262 and 263 of Criminal Code are incriminating acts, also related to cybercriminal, such as:

- Counterfeit and abuse of credit cards and cards for non- cash payment;
- Creation, acquiring and providing to other persons with means for counterfeiting;
- Issuing insolvent checks and non-cash payment means;

Provisions of the **Criminal Procedure Code** (»Official Gazette of Montenegro«, No.57/09), are addressing issues regarding conducting of criminal investigations, on the first place interception and control of communications on the internet, cross border access to the information, as well as modalities for conducting verification of Internet users in emergencies.

Criminal Procedure Code is aligned with international law, whereas its provisions are aligned with certain procedural provisions in the area of cybercrime, regarding the European Union. Especially important are provisions of the Code, related to protection of national economy in framework of contemporary trends of information society. In this regard, the area of data encrypting by the final user or legal entities (virtual private networks and similar), is particularly important, as well as the area related to contemporary approach to company financial audit, bearing in mind that it is being inevitably transferred in electronic domain, in accordance with the process of computerization of all business subjects (regulations on keeping e-mail, e-transactions, storage of crypto keys and similar).

Law on electronic signature (»Official Gazette of Montenegro«, No 55/03) regulates usage of electronic signature in legal transactions, administrative, judicial and other proceedings, as well as rights, obligations and responsibilities of physical and legal entities in relation to electronic certificates. In accordance with provisions of this Law, advanced electronic signature, which can be verified on the basis of qualified certificate, in relation to the electronic data, has the same legal force as own personal signature, i.e. personal signature and the stamp in relation to the hard copy data, and it is certainly admissible as evidence in legal matters. Law in particular defines obligation to ensure safety of instruments for creation of advanced electronic signature, as well as that advanced electronic signature should be protected from counterfeiting using of currently available technology (Article 10). At the same time, the Law provides that data for creation of advanced electronic signature can be reliably protected from unauthorized use (Article 11). In that sense, means for verification of advanced electronic signature are means that provide:

- Reliable determining that data used for verification of electronic signature correspond to data presented to a person who carries out verification;
- Reliable verification of signature and correct displaying of the verification results;
- Reliable insight into the content of signed data;
- Reliable verification of authenticity and validity of signatory's certificate at the moment of signature verification;
- Correct displaying of signatory's identity;
- That any amendment to signed data can be reliably identified.

Article 12 of the Law on Electronic Signature foresees that Republic administration authority competent for information technology affairs shall regulate: electronic signature and advanced electronic signature protection measures; Signatory's identity verification measures; technical-technological procedures for creation of advanced electronic signature; as well as the conditions that means for creation of advanced electronic signature shall fulfil.

This Law also foresees special provisions for protection in case of certification service providing, where Article 14 of the Law stipulates that certification service provider can perform this services if he has system of physical protection of devices, equipment and data as well as security solutions for protection against unauthorized access to and damage of information. Additionally, certification service provider has to have system for storage of all relevant information relating to qualified certificates, to own secure system that prevents saving and copying of data for creation of electronic signature for persons to whom certification services are provided; systems for physical protection of devices, equipment and

data, as well as security solutions for protection against unauthorized access as well as to use reliable system of keeping qualified certificates.

Law on Electronic Signature stipulates obligation of signatory to carefully store means and data for creation of electronic signature from unauthorized access and use, and duty to immediately seek the revocation of his/her certificate in all cases of loss or damage of means or data for creation of own electronic signature. This Law also foresees sanctions in cases of unauthorized access and usage of data and means for creation of electronic signature and advanced electronic signature, as well as sanctions in case of infringement by signatory himself, or his/her representatives, or certification service provider (Articles 42-44).

On the basis of Law on Electronic Signature (»Official Gazette of Montenegro«, No 55/03), Ministry for Information Society and Telecommunications has adopted **Rulebook on Electronic Signature and Advanced Electronic Signature Protection Measures** (»Official Gazette of Montenegro«, No 61/2011). Rules are setting measures for protection of electronic signature and advanced electronic signature, measures for verification of identity of signatory by signatory himself or certification service provider in Montenegro, technical-technological procedures for creation of advanced electronic signature and conditions which means for creation of advanced electronic signature should fulfil. All measures for protection of electronic signature and advanced electronic signature, procedures for creation of advanced electronic signature, conditions that means for creation and verification of advanced electronic signature should fulfil, are aligned with international standards (which are also listed in Rulebook). Rulebook is stipulating that signatory, in order to protect electronic signature and advanced electronic signature, from unauthorized access, theft or damaging, uses passwords, PIN codes and other types of protection of electronic signature. If signatory loses or mean for creation of electronic signature, or this mean is stolen from him, Rulebook foresees obligation of signatory to immediately inform certification service provider and submits request for revoking or suspension of his certificate.

Particularly important are provisions of the Rulebook regarding storage and protection of data for creation of advanced electronic signature of certification service provider, which stipulate implementation:

- Of means for creation of advanced electronic signature in accordance with American standards FIPS140-1 (set by the standardization body: National Institute of Standards and Technology - Federal Information Processing Standards), of sufficiently high level - not lower than level 3; or in accordance with standard FIPS140-2, which provide work with data for creation of electronic signature;
- Data for creation of signatures by application of RSA or DSA algorithm of at least 2048 bit longitude, or adequate level of Elliptic Curve algorithm, SHA1 or SHA-2 (SHA-224, SHA-256, SHA-384 i SHA-512);
- Cryptographic algorithms (3DES algorithm - 128 bit or AES technique) for data access protection
- Certification service provider protects data for creation of electronic signature in accordance with determined rules and international standards in order to prevent physical or electronic access to these data by unauthorized persons.

Ministry for Information Society and Telecommunications has adopted ***Rulebook on the Content and Manner of Keeping Records and Register Of Certification Service Providers*** (»Official Gazette of Montenegro«, No. 71/10 from 03/12/2010) which regulate the content and manner of keeping records of certification service providers, the manner of registry keeping of accredited certification service providers; as well as the minimum amount of

insurance against the risk of liability for damages that may occur during the performance of certification services.

On the basis of Article 12 paragraph 2 and Article 33 paragraph 2 Law on Electronic Signature (»Official Gazette of Montenegro«, No.55/03), Secretariat for Development has adopted ***Rulebook on Measures and Procedures for Usage and Protection of Electronic Signature, Means for Creation of Electronic Signature and Certification System,*** which regulates measures, procedures and forms of protection of electronic signature, and advanced electronic signature, means for creation of electronic signatures, protection of certification system and data on signatory, as well as procedures of signatory identity verification during issuance of electronic certificates in Montenegro.

Rulebook defines obligation of alignment of procedures for creation of electronic signature, criteria which should be met by means for creation and verification of electronic signature, with corresponding international standards and recommendations:

- Technical standards of ETSI (European Telecommunications Standards Institute) and ESI (Electronic Signatures and Infrastructures);
- European standards CEN/ISSS and documents CWA (CEN Workshop Agreement);
- EESSI SG standards (European Electronic Signatures Standardization Initiative Steering Group);
- IETF RFC (Request for Comments) documents;
- PKCS (Public Key Cryptographic Standards) documents and recommendations of RSA Data Security company;
- European Common Criteria (for Information Technology Security Evaluation) in part EAL (Evaluation Assurance Level);
- American standards FIPS 140-1 (determined by standardization body: National Institute of Standards and Technology -Federal Information Processing Standards), as well as FIPS 140-2 standards.

The Rulebook at the same time prescribes that signatory is obliged to protect data for creation of electronic signature from unauthorized access, alienation and irregular use. Protection should be additionally provided by usage of a password, biometric procedures or other protective techniques.

Also, Rulebook defines obligation to certificate service provider, who issues qualified certificates, to adjust equipment for verification and functioning of certification system, with technical standard FIPS 140-1 of sufficiently high level– at least level 3, i.e. with determined common model for protection of program-technical and informatics equipment and systems »Common Criteria 2.1« based on ISO 15408-1:1999 standard. Certificate service provider, who issues qualified certificates, has to adjust procedures and forms of system protection with currently valid recommendations and standards in area of protection and safety of information systems and means functioning. Finally, Rulebook regulates that certificate service provider, who issues qualified certificates, has to adjust system of certification and information system with demands of information systems security, in accordance with models ISO/IEC 17799:2000 (Code of Practice for Information Security Management) and BS 7799-2:1999 (British Standard for Information Security Management – Specification for Information Security Management System).

Information Secrecy Act (»Official Gazette of Montenegro«, No.14/08) defines types and degrees of confidentiality of information as well as measures and procedures for the

classification, access, storage, handling, and protection of classified information. According to his Law, secret information are information which disclosure to unauthorised person would have or might have adverse effects on security, or political or economic interests of Montenegro, and is related to: defence; national security; foreign affairs; intelligence and security activities of the State agencies of Montenegro; scientific, research, technological, economic and financial affairs of importance to the public security, defence, foreign affairs and public security , and intelligence and security activities of the State agencies of Montenegro and systems, appliances, projects and plans of importance to the defence, public security, foreign affairs and intelligence and security activities of the State agencies of Montenegro. Secret information is assigned with one of following degrees of confidentiality: top secret; a secret; a confidential, restricted. Modalities and methods of labelling secrecy of information are prescribed by the Government of Montenegro.

Secret information labelled with »top secret« »secret« and »confidential« can be accessed only by person, which was issued a permit for access to secret information, on the basis of conducted security check. Exceptionally, access to secret data without permit for access to secret data is granted to certain number of people determined by this Law, but only access to that secret information which are necessary for implementation of their authorities. Access to secret information with label »restricted« is granted to all employees of the state body or organization. Secret information of foreign countries or international associations, keep labels for degrees of secrecy which are in use in those states or associations. Permission for access to secret data is issued by Directorate for Protection of Secret Data, on the basis of security assessment, done by Agency for National Security, in accordance with the Law.

Public administration bodies, as well as legal and physical entities, when they discover secret data in implementation of their legal duties or execution of contracted work, are obliged to behave in accordance with the Information Secrecy Act.

Law on Free Access to the Information determines conditions under which is possible to exercise the right on access to information in possession of state bodies. This right is granted to any national or foreign legal or natural person, in accordance with the Law. However, right to access to information doesn't exclude the necessity for protection of these information and care for their safety. In this sense, in cases determined by this Law, state bodies can restrict the right to access to the information. Right to free access to the information is granted through direct inspection of public records or the original or a copy of such information, within the premises of the government agency, transcribing such information by the person that submitted the request for such information, within the premises of the government agency, or by submitting of a photocopy of requested information. Free Access to the Information Demand should be submitted in written form, directly, via regular mail, or electronically.

3.2 Cyber Security Strategy

Having in mind that strategic goal of Montenegro is building of integrated, functional and efficient cyber space, in accordance with international standards and principles, Montenegro has adopted **Cyber Security Strategy**, in July 2013, for period of 2013-2017. Strategy clearly

defines aims and priorities, and represents vision of Montenegro in terms of cyber security and its granting. On the basis of this strategy, Montenegro has adopted annual Action Plans.

Strategy defines following concrete activities, which should be implemented in following period by key decision makers:

- Set the vision, scope, aims and priorities;
- Follow risk assessments on the national level;
- Take into consideration existing policies, regulations and capacities;
- Develop clear managing structure;
- Identify and include interested parties;
- Set confidential mechanisms for information exchange;
- Develop cyber safety plans for unforeseen emergencies;
- Organize cyber security exercises;
- Set up basic security demands;
- Develop mechanisms of incident reporting;
- Increase awareness of citizens on this issue;
- Nourish cycle of research and development;
- Strengthening capacities through trainings and advancement programs;
- Set up incident response capacity;
- Respond to cybercrime;
- Engage in international cooperation;
- Set up public-private partnerships;
- Balance between security and privacy protection;
- Conduct evaluation;
- Align National strategy on cyber safety.

At the same time, the Strategy defines key risks, challenges and threats for cyber security in Montenegro:

- Weaknesses in organization of cyber protection can represent danger for national security of Montenegro;
- Internet in Europe and in our close surroundings is intensively being used in criminal purposes, for drug trade, money laundering and financial frauds, thus Montenegro won't be spared of this danger;
- ICT infrastructure, computer systems and users in Montenegro are exposed to majority of cyber dangers and attacks which affect rest of the world. This includes malicious programs, electronic frauds, web defacement and »hacking« of electronic mail;
- Underdeveloped cooperation between private and public sector in area of coordination of security systems of risky infrastructure;
- Inexistence of procedure of registering incident situations in the cyber space of Montenegro;
- Inexistence of National Council for Cyber Safety with its functions;
- Cyber space is increasingly used for organization and media propaganda of extremist and radical groups, which promote their activities in this way, recruit new members, organize terrorist actions and in such manner, represent a threat for national safety in Montenegro.
- Piracy contributes to high rate of infections by computer viruses;

- On-line manipulations, using social engineering through e-mail messages, such as »Nigerian 419« fraud, phishing, go hand in hand with identity theft (illicit procurement of accounts and passwords of other users). Such situation in Montenegrin cyberspace is concerning and problematic, not only for Montenegro, but also for other countries. Montenegrin citizens have been victims of fraud in the past and lost large amounts of money;
- In period 2008-2013, attackers have altered or taken control over more web pages of Montenegrin institutions;
- In Montenegro, in the last period more attacks on information system was recorded, on services of internet providers and on the bank sector;
- In the previous years a significant number of cases where attackers have taken control over user profiles of Montenegrin citizens on social networks and left inappropriate messages, in order to compromise profile owner, has been recorded.
- 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;
- 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;

Cyber Security Strategy defines seven key aims:

1. Defining institutional and organizational structure in the field of cyber security in the country, which encompasses establishment of National Council for Cyber Security and creation of local CIRT teams;
2. Protection of critical information structures in Montenegro, which encompasses insurance of structure and resources necessary to provide cyber security;
3. Strengthening of capacities of state bodies to implement the law;
4. Strengthening of capacities and possibilities to provide adequate response in incident situations;
5. Strengthening of the role of Ministry of Defence and Montenegrin Army in cyber space;
6. Strengthening of public-private partnerships;
7. Raising awareness of society on Internet protection.

4. Cyber security Education in Montenegro

4.1 Formal education on Cyber security at select Higher Education Institutions

Programs at all levels at HEIs (undergraduate, graduate, Master and Doctoral) should be checked at three universities:

4.1.1 University Mediterranean

Faculty of Information Technology of University Mediterranean, is a modern academic institution that educates professionals to perform activities in the field of information technology. It aims to industry, government agencies and financial institutions provide a high level of staff knowledge and competence in the field of information technology.

The curriculum is designed according to Europe's leading faculty in the field of computer science where they used the experience to date in our country. Lecture, exercises and professional practice are designed to allow for the formation of highly educated people who are willing to answer the high demands of the world market. The curriculum, as well as the entire process of teaching is aligned with the principles of the Bologna Declaration.

The Faculty of Information Technology is taught an Information Technology degree program with three modules, namely:

1. Information Systems
2. Software Engineering
3. Computer networks and telecommunications

The first four semesters are common for all three directions, and in the fifth semester, students select one of the available routes

Teaching is aligned with the current needs of the economy for skilled IT personnel, so that during the study allows students to obtain certificates of large international companies that are recognized throughout the world (Microsoft, Cisco, Oracle, Cambridge, and ECDL). These diplomas provide evidence that our students have the knowledge equivalent to the knowledge that provide the world-famous colleges in this area. For teaching are engaged in domestic and foreign professors who have prospered as the leading experts in certain areas.

There is no many courses considering cyber security at the Mediterranean University at the moment. As very young topic it is only considered at the Faculty of Information Technology through the courses Security and protection of information systems and Security and protection of computer networks. Both of the courses are at the undergraduate level of studies. The courses cover basic topic from the area of information systems security, software security and network security. Students are introduced to basic routines how to manage their information systems, regarding security of the access, security of the networks, security of data flow, security of data stored in the system and security of the personal data belonging to different users. Also students are introduced to ways of possible attacks to networks behind

information system. They will learn how to recognize risks in communications, means of stealing data, entering the system, hacking or spying it. Also they will learn how to prevent most common types of attacks and how to improve system security. Other course is about security of software. The idea of whole course is that after security of information system is breached next level of protection is at the level of application-software. This is very important for the inside attacks. Students learn how to protect operation systems at workstations, how to protect single application and how to enable multiple users to access single application on a single work station and how to protect it. Students also learn how to use third part solutions to fight malware and viruses. This is basic education that merely scratches the cyber security area.

4.1.2 University Donja Gorica

Forms of formal education in the field of cyber security at the University of Donja Gorica

The University of Donja Gorica, due to the rapid development of information networks in recent years and the significant need for education professionals in the field of information security, has launched post-graduate programs in this field. In fact, at the University of Donja Gorica, there are two post-graduate study programs:

- Postgraduate academic study program (master studies) »Cyber Security« - master program established at the Humanistic studies;
- Postgraduate academic study program (Postgraduate and Master Studies), »Data protection and Security of Information Systems« - involves a two-level program of study that is being developed at the Faculty for Information Systems and Technology.

Study programs in the field of cyber security that are being developed at the University of Donja Gorica are very important form of formal education that provide a high quality and systematic education system, especially needed in the process of fulfilling obligations in this area, deriving from the integration process of Montenegro in EU and NATO organization, that posed an urgent requirement for establishing and measure of information security of each country, potential members. In fact, it is evident that in all countries of the region, as well as in Montenegro, information space is imperilled.

However, the situation in Montenegro is further unsatisfactory because of the fact that there is not established adequate technical and semantic infrastructure, and many problems are still not evident. The entire IT space is at a high risk of violation of information security, due to the fact that it has being developed and implemented short-term measures to eliminate security vulnerabilities, rather than long-term planning and coordinated actions. At the same time, a significant problem is the lack of basic knowledge and research in this area, as well as the lack of experts in this field. Accordingly, it is important to increase the number of specialists and researchers in the field of cyber security at the universities, institutes, research centres and the private sector, as well as to increase investments in education and acquisition of knowledge that is essential in all aspects of information and communication technologies, in order to raise the general level of cyber security. Large companies and government organizations constantly need experts in this filed, against the small companies that need their occasionally engagement for the assessment of the security risk, establishing protection measures and techniques and solving specific problems.

Postgraduate academic study program »Cyber Security«

Humanistic studies develop postgraduate Master study program »Cyber security«, which is aimed at educating the next generations of experts in the field of cyber security, which is implicitly promotes the development and research capacity in this area. The main objective of the multidisciplinary master study program »cyber security« is the development of human resources and the establishment of the quality system of cyber security in all organizations and institutions, both private and public sector, thus raising the level of national security to a higher level.

This program focuses on the study of several important characteristics of cyber security: global and multidisciplinary aspects of cyber security, diversity of forms and the appearance of a wide range of potential target, providing a comprehensive understanding of the concept of security and its implications. Specific areas of research include the area of security, ICT, economics and international law. This master program creates experts who will be able to adequately analyse threats of cyber-attacks, organize and establish an adequate system for cyber protection, and operate the system of cyber security by ensuring the continuity of the business process in the private and public sectors.

This master program is aimed at preparing students for fallowing tasks, responsibilities and professions:

- Head of the department of information security in the private and public sectors;
- Expert for testing and auditing of security systems;
- Consultant for computer security in business and government organizations;
- Expert in legal matters in the area of cyber security.

Postgraduate master program »Cyber security« is basically intended for all students who wish to accumulate the most important knowledge in the field of cyber security as well as from in several related disciplines. Consequently, the concept of the study program will enable graduates, due to the knowledge acquired, to profiled themselves in serious experts of these areas in the state or private sector.

In the curriculum of master program, there are following key subjects:

- International and national security;
- Managing cyber security;
- The modern cyber security challenges and technologies;
- Cybercriminal;
- Digital Forensics;
- Introduction to cryptography and security mechanisms;
- Legal and ethical aspects of cyber security;
- International Terrorism (theory and practice).

Postgraduate academic study program »Data protection and Security of Information Systems«

Postgraduate academic program (postgraduate and master) »Privacy and Security of Information Systems«, involves a two-level program of study at the Faculty of Information Systems and Technology, University of Donja Gorica. The specialist's and master's study program, which has being developed for several years, contributes to satisfy the demand for information security experts who possess a balanced analytical skills and business acumen. In

this regard, the program combines security politics, management and technology aspects of information security as well as risk management.

The initial goal of the Faculty of Information Systems and Technology was the establishment of a high-quality degree program that will attract young perspective people for educating them in IT security that is required to private companies, the state, government and higher education, and science. Through the organization of several generations, this program has, by content and quality, become recognizable in the European environment, while at the same time has become very important for the private and public sector in Montenegro and wider region.

Postgraduate program »Privacy and Security of Information Systems« is intended to the following students:

- Students who want to continue graduate studies, after completed studies at the University of Donja Gorica;
- Engineers (educated at different universities) that for some time working in this field and they need to improve and systematize their knowledge;
- Lawyers in charge for data protection in their companies, who want to upgrade their IT knowledge and learn IT standards and norms in the field of data protection.

In the curriculum of master program, there are following key subjects:

- Subjects that provide the nucleus of the profession, technical aspects (e.g. introduction to cyber security, data protection, protection of information networks, digital forensics, risk management);
- Subjects that cover legal and social aspects (e.g. Cyber Law - Computer Law, safety standards in IT);
- Subjects needed to raise the knowledge of the IT environment where lurking danger, in which IT protection is offered (Internet banking networks - advanced level, database - administrator access, modern technology - virtualization, cloud area).

Within this postgraduate study program, it has been studied the methods of assessing of security risks, establishing measures and protection techniques in IT and solving specific problems. More specifically, the key learning outcomes are:

- Knowledge and understanding of the role, the foundation, the concepts and structures of data protection and security of information systems;
- Practical skills and knowledge about methods, techniques and software tools for the protection of information systems;
- Practical knowledge and skills in the use of modern application software solutions artificial intelligence, expert systems, DSS - decision support systems and knowledge management systems;
- Knowledge of digital forensics;
- The use of information systems in the management of business changes;
- The use of information systems in the risk management;
- Knowledge of international standards in the field of security of information systems;
- Practical knowledge in the field of e-business;
- Knowledge of IT audit;
- Practical knowledge of project management;
- Knowledge of cyber and computer law.

4.1.3 University of Montenegro

University of Montenegro is the biggest and only state University in Montenegro, with a more than 21000 students, but has not the independent study program related to Cyber security at any level - undergraduate, graduate, Master or Doctoral. As relevant faculties for Cyber education at University of Montenegro four faculties are taken: Faculty of Law, Faculty of Political Science, Faculty of Science and Faculty of Electrical Engineering.

Faculty of Law

At basic studies at Faculty of low, on the 4th year, at Criminal department, exist subject »International criminal law«, but this curriculum does not cover themes related to cyber security.

On the other side, specific three year study program at Faculty of law – Criminology and security, that should study defence policies and protection strategies from cyber-attacks, just mentioned these issues within the lectures on the following subjects: National security, Security management, Security systems on the 3rd study year.

Master and doctoral studies do not content any subject that process cyber security themes.

Faculty of Political Science [1]

At Faculty of Political Science basic, specialist and master studies are organized in five departments – International relations, Political science, Journalism, Social policy and social welfare, and European studies. A doctoral study does not organize at department of European studies.

In the 5th semester of basic semester at department International relations and European studies, subject »NATO and collective security systems« is in the curricula, but this subject does not cover any issues related to cyber security. The same situation is with the subject »EU foreign and security policy« in the last semester of specialist studies at department of European studies.

Master and doctoral studies do not content any subject that process cyber security themes.

Faculty of electrical engineering [2]

At Faculty of electrical engineering there are two separate programs at all levels of studies (basic, master and doctoral) – Electrical engineering, telecommunications and computers; and Energetic and automatic, with a few different departments. Although, subjects related to ICT exist at both study programs, they are more oriented at programming and not research cyber security area.

Also, at Faculty of electrical engineering, Applied computers is organized as the separate undergraduate and graduate program, with main goal to provide quality, special educations in computer science. At this programme, in 4th semester subject »Data and system protection« found its place. This is the only one subject at Faculty which curricula covers cyber security issues.

Faculty of science [3]

Study programs Maths and Maths and computers from Faculty of science are taken as relevant for cyber security education. After analyse their curriculums at all levels, we could not find any subject which covers cyber education, even at PhD studies in Computing. Existing subjects are much more based on programming, data basis, but not on their protection.

Two separate undergraduate and graduate programmes are organized at this Faculty, such as: Computer' studies and Computing and information technology. Both of them provide one course about cyber security, as follows:

- Computer' studies – subject »Security of computer systems« – 4th semester
- Computing and Information systems – subject »Data protection« – 2nd semester of specialist studies.

4.2 Informal education on cyber security

In Montenegro, companies, especially SMEs, usually don't have a practice to organize security trainings for their employees. In the last time, the growing trend of cyber training organization is noticed in the large companies. A short description about it is given in the following text.

Sava Montenegro osiguranje

»Sava Montenegro osiguranje« is insurance company that provides services of life insurance in the Montenegrin market for more than a decade. It is the second largest insurance company in Montenegro, with a market share of about 20% and more than 160 employees.

In the »Sava Montenegro osiguranje« company organization of security trainings is regular practice. This company s formal, obligated trainings, and more often informal trainings, in which employees through regular daily work present best practices that must be followed in working with computer equipment and data. Also, »Sava Montenegro osiguranje« had adopted procedures and regulations, which are regularly presented to employees, and practically demonstrated their usage in the staffs' daily work.

Protection measures are carried out through forcing the aforementioned rules written in procedures and by training organization.

Hypo Alpe Adria bank

»Hypo Alpe Adria Bank«, as one of the very important actor on the Montenegrin bank market, has recognised that development, exploitation and protection of information assets are critical for the long-term competitiveness and survival of the company and the entire industry. Thus, protection of information assets assumes the primacy than the physical and logical protection of resources.

IT security in Hypo Alpe-Adria-Bank AD Podgorica is based on international standards ISO27001 and ISO27002. Decision of the Board of Directors about security at the Hypo Alpe-Adria-Bank AD Podgorica is based on international standards and their full technical and organizational implementation, and published in Policies and Procedures. In line with that, Hypo Alpe-Adria-Bank AD applies technical and organizational protection measures as part of the overall management system, based on a business risk approach, for establishment,

implementation, monitoring, reviewing, maintaining and improving information security based on ISO27001: 2005. An important factor in the overall safety in the company is that employees have trained for the proper handling with information assets.

Lovćen osiguranje

Lovćen osiguranje is the first insurance company in Montenegro, and leading insurance company by collected premium, market share and capital.

This company has a centralized anti-virus and modern firewall system that controls the network and provides security at multiple levels. Employees are not administrators on their computers, so they cannot install anything without the permission of the employees in IT. Assessment to the system has defined by implementation strong password policies in accordance with current standards.

In the last, several years, employees has received on their mail the »Security awareness« document, which lists and describes various dangers that lurk in the cyber world, and advices what they can do to protect themselves. The document also describes how to protect the password from theft, unauthorized access to their data, on the best way.

UNIQA osiguranje

»UNIQA osiguranje« is the insurance company which performs in Montenegro since 2008, which covers life and general insurance.

UNIQA does not organize trainings related to cyber security for its employees. The main reason for that is because its information system is protected from unknown falls and access to locations that are not work-related or not safe by a firewall and proxy server.

Atlas bank AD Podgorica

»Atlas bank« is a member of big Atlas Group and one of the leading business banks in Montenegro. It started its business in April 2002 and very soon gained the reputation of a reliable business partner.

Atlas bank has organized trainings for its employees related to cyber security and protection measures. Giving great importance to cyber protection issues, this year, Atlas Bank has adopted Plan how to raise awareness about the information systems' safety. According to the plan, all employees should be trained how to react in case of cyber-attacks. Until now, the most of employees has passed the necessary training, and the rest will do so as soon as possible. This Plan envisages continuous staff training and constant monitoring of results, in order to raise staff competences about cyber security at the highest possible level.

In addition to the training, bank constantly use other formats (via e-mails, etc.) to familiarize employees about cyber security, safe way of using the internet, the dangers at the Internet, risks and so on.

Atlas bank AD Podgorica

»Atlas bank« is a member of big Atlas Group and one of the leading business banks in Montenegro. It started its business in April 2002 and very soon gained the reputation of a reliable business partner.

Atlas bank has organized trainings for its employees related to cyber security and protection measures. Giving great importance to cyber protection issues, this year, Atlas Bank has adopted Plan how to raise awareness about the information systems' safety. According to the plan, all employees should be trained how to react in case of cyber-attacks. Until now, the most of employees has passed the necessary training, and the rest will do so as soon as possible. This Plan envisages continuous staff training and constant monitoring of results, in order to raise staff competences about cyber security at the highest possible level.

In addition to the training, bank constantly use other formats (via e-mails, etc.) to familiarize employees about cyber security, safe way of using the internet, the dangers at the Internet, risks and so on.

Montex elektronika

Montex elektronika is a company whose primary activity is the design, implementation and maintenance of information systems, with particular emphasis on information security.

Extensive experience of Montex has shown that education is of great importance, and therefore it occasionally organizes informative presentations and workshops for their clients. However, the fact is that computer literacy in Montenegro is still at low level, compared to international standards, and thus the additional training is required.

This company tries to inform its customers and introduce them the terms such as virus, anti-virus protection, SPAM, security policy, secure access, potentially malicious applications, backup and so on. On the other hand, Montex gives advices and recommendations to the customer how to preventive react, and avoid acting after the incident.

In opinion of Montex representatives is that the users (in general) are becoming more aware of the problems that may arise as a result of irresponsible conduct of ICT services, but it is not at satisfactory level, and that they should be further informed about the basic principles of protection (do not leave personal information the sites, do not use credit cards for payment on unreliable websites, do not use unprotected wireless network to access relevant information, e-mails, and much more ...)

Telenor

Telenor is the leading provider of mobile telecommunication services in Montenegro. It was the first mobile operator in Montenegro when started writing the history of mobile communication from 1996.

Based on the fact that information is one of the most important resources, their protection is the top priority of Telenor. Since its establishment, Telenor paid a lot of attention to this segment, as on protection its own systems, as well as on respect of fundamental principles of information security during the development and implementation customer services. A framework for drafting local policies and procedures, and measures of information assets protection is an international standard ISO/IEC 27001. Also, attention is directed to the employees, so in the initial training of new employees is training related to information security. Every year, Telenor Group initiates various campaigns aiming to raise awareness in this area.

Central bank of Montenegro

Central Bank of Montenegro is the main monetary authority in Montenegro. Central Bank of Montenegro has always paid special attention on information security. Council of the Central Bank had adopted the »Basic policy document for protection of CBM information system« in 2004. Existence of the policy, as well as the obligation to comply the formal procedures in the performance of all business activities, has helped to create a considerable level of information security culture of its employees.

Among the first in Montenegro, in 2008, CMB has implemented a corporate PKI (Public Key Infrastructure) solution, which enables two-factor protection while logging on to the computer (by using a USB token), encryption of documents and e-mails. In addition, CBM has implemented the appropriate protection systems of computer networks, including Firewall, Vulnerability Scanner and Intrusion Prevention Systems.

In the middle of 2012, Central bank has begun the process of harmonization with the leading international standard for information security management ISO/IEC 27001, with the aim to comply information security management in the Central Bank with best practice. Implementation of standards is done independently, guided by staff who had the necessary education, experience and relevant certifications in this field (CISM, ISO/IEC 27001 Lead Auditor, ISO / IEC 27001 Internal Auditor).

Also, the »Information security policy of the Central Bank of Montenegro« has been adopted, and training for all employees was organized in order to present new established rules. All employees were required to sign a statement of understanding and acceptance of information security policies, after completing training.

An internal team for implementation ISO/IEC 27001 standards had formed. The team had built from representatives of all organizational units and performed more than one year. Their performance resulted by the harmonization of information security management to the standards, and creation of framework for managing information security risks, which included a comprehensive risk assessment at the central bank. These activities have additionally strengthened the awareness of CBM employees about importance of information security.

4.3 Cyber security education for the broader public

Ministry of information society and telecommunications of Montenegro (MIST) is recognized importance of cyber security and adopted The Cyber Security Strategy for Montenegro 2013-2017. This Strategy anticipates measures for raising awareness [4].

In order to ensure safer Internet environment for Montenegrin citizens and raise their knowledge about cyber security, Ministry planes to organize trainings for the boarder public. Special attention will be given to children and youth, and continuous introduction of new programmes of cyber security at all levels of education.

MIST in cooperation with Ministry of education has already started with informal education of children in primary schools about cyber security. Also, MIST and Telenor Company realized project named »Splitting generations – safe Internet for future generations« in the September 2012. This project was public-private partnership and aimed to raise awareness about using information technologies, education and safety Internet surfing for children.

In the next period MIST is planning to continue to organize projects and campaigns for promotion of safe Internet using with special focus on child protection.

MIST, together with the Ministry of Education and universities in Montenegro, works on organizing special programs from the area of cyber security with the aim of creating staff with highly specialized knowledge from this field.

5. Cross-matching between EU practice and current practice in Montenegro

When comparing the current status of cyber security in Montenegro with EU practice, it appears evident that there is a gap to fill. The Montenegrin society is in full transformation, and all public and private organizations are making a notable effort to rapidly meet EU standards in terms of making the population understanding the risks, and constituting a workforce able to put in practice suitable countermeasures. In the following, we will exhibit a concise cross-matching between EU practice and current practice in Montenegro for cyber security, trying in particular to identify what aspects require to be quickly and carefully addressed to meet the EU standards.

5.1 Cyber security standards and frameworks

In recent years, Montenegro made remarkable efforts to meet the EU standards for cyber security. As a stepping stone, the government defined:

- A novel legal framework, including cybercrimes under all possible forms;
- »The Strategy in Cyber Security of Montenegro from 2013 to 2017«, that is, a plan for National cyber defence in the upcoming years

Formally, from this perspective Montenegro seems to already have reached the most common standards in place, probably due to the fact that similar aspects are among the easiest one to adopt by simply taking inspiration from EU countries.

However, it is fundamental to fill the gap between plans and actions as soon as possible: the principles identified in the National Strategy need to be put in practice, and the law enforcement agencies need to be given all instruments necessary to be able to tackle the newly identified forms of cybercrime.

To this end, we identify the following steps that need to be urgently addressed:

- **Clarify the role of the military in (national) cyber security**: while Montenegro has identified that the military must have cyber security capabilities, these capabilities are not well defined nor adequately covered by resources
- **Define inter-ministerial bodies appointed to coordinate the actions of different governmental institutions**: among the main aims of the National Cyber Security Strategy there is »Defining institutional and organizational structure in the field of cyber security in the country, which encompasses establishment of National Council for Cyber Security and creation of local CIRT teams«; nothing similar has been created yet, and different ministers and governmental bodies have been given duties concerning cyber security that often overlap; it is fundamental to identify a guidance able to distribute responsibilities and workload
- **Improve collaboration between public and private institutions**: the importance of implementing long-term and well established agreements between private

organizations (usually able to provide a more skilled workforce) and public institutions is vital to guarantee a top-level protection against ever changing cyber attacks

The legal framework seems well structured and elaborated. However, it is not clear to what extent it is in line with the EU regulations and directives in the field. For example, while it tackles electronic signatures, it is not clear if it implements the related EU directives and how.

5.2 Cyber security Education in Montenegro

Many universities in the EU are in the process of setting up a cyber-security curriculum. Often these curriculums are interdisciplinary, as is the case in Montenegro. This is especially true for smaller countries, where the same curriculum is expected to deliver cyber security managers as well as technical experts. Once specialized PhD and Master's programs have reached a stable state, the cyber security education is going to flow to lower levels of education and to other fields of education.

Trying to identify the most important issues in formal education in Montenegro, and the most relevant differences with EU practice, we come to the following:

- **Lack of experts**: in general, it seems that Montenegro is missing a pool of experienced professionals and teachers, able to both define new cyber-security curricula, and to teach related subjects.
- **Lack of specific courses**: the only state University in Montenegro seems to completely lack any course of cyber-security. While it is somehow acceptable not to have a cyber-security curriculum yet, it is extremely urgent to identify some basic inter-disciplinary courses (e.g., cryptography, system security, network security) and to put them in practice as soon as possible.
- **Lack of basic knowledge**: Even in UDG, where two specific curricula for cyber-security experts are already in place, it seems that not enough importance is given to basic knowledge which is fundamental to build a skilled workforce. The curricula seem to be only focused on law and technological aspects, but there is a whole set of knowledge that is needed to have a deep understanding of many cyber-security threats, ranging from mathematics (e.g., cryptography, graph theory, load balancing) to physics (e.g., waves propagation, energy consumption and harvesting).

Informal and broad public education

Informal training within companies and public campaigns supported by the government are encouraging, but the niche of private cyber security training companies seems to be conspicuously vacant or omitted.

The foreseen awareness campaigns probably do not require to be guided by experts with very advanced technological competences.

To the contrary, education in SMEs needs skilled professionals for:

- Organization and planning
- Courses delivery
- Final examination and reports

Even if Montenegro is promisingly developing a local workforce that will be probably able to take care of the aforementioned duties in the next future, it is fundamental to subsidize collaboration with public and private organizations from EU countries to be able to start extensive courses and workshops as soon as possible.

The following table recaps how the Montenegro education system compares to the EU practice for cyber security education as described in Deliverable 1.2.

Formal education on cybersecurity	
Bachelor study programmes	It seems that no Bachelor study program on Cyber Security is provided. A full bachelor programme devoted to cyber security may not be necessary, as long as that other courses provide notions on this topic. However, it seems that bachelor programmes does not cover specific cyber security notions.
Master study programmes	Some Universities in Montenegro provide specific master study programmes on cyber security with a multidisciplinary approach and with different cyber security expert profiles.
Doctoral study programmes	It seems there is no PhD programme specific for cyber security. A specific PhD on cyber security may not be required as long as other PhD programmes (e.g. Computer Science) cover the topic and provide the same profiles. However, it is not clear if this is the case.
Informal education on cybersecurity	
Professional trainings	It seems that only few initiatives or general professional training at national level provide notions of cyber security for a broad spectrum of professionals dealing with ICT (e.g. *GenSet Cybersecurity* by IMTM). It is not clear if some private company operating in the field provide professional courses on cyber security, and to what extent other foreign programs (e.g. SANS) are spread and accessible.
Domain specific training	It seems that only few private companies concerned with cyber security threats provide employees' training on this subject.
Cyber security education for the broader public	
Rising awareness campaigns	It seems that effective and broad campaigns are not available.

Informative campaigns on cyber security	It seems that effective and broad campaigns are not available. Primary schools and high schools do not provide information about a conscious use of ICT and the Internet with concerns about cyber security. Several initiatives between Universities, private companies, and schools should be organised.

6. Conclusion

Each state is obliged to protect its own IT infrastructure, as well as its cyber space, which covers the national domain. To this end a strategic interests of Montenegro is to build an integrated and functional cyber space in accordance with international standards.

With regard to its foreign policy priorities - full membership in EU and NATO, providing the prescribed safety criteria at the relevant EU legislation, becomes a priority of Montenegro.

Building of the relevant organization and institutions, improvement of legislation, are the most important development trends of the cybersecurity in Montenegro.

Establishment of the National CIRT at the Montenegro Ministry of Telecommunication and Information Society, made a big step towards preventing and eliminating cyber threats affecting the state and its citizens, according to Strategy cyber security of Montenegro until 2017, which was adopted by the Montenegro Government in 2013.

CIRT Government adopted the Strategy for the cyber security of Montenegro until 2017. National CIRT is a central point for coordination and exchange of data, cyber defence and elimination of the consequences of cyber security incidents in the territory of Montenegro. CIRT in cooperation with key institutions in Montenegro deals with the detection, monitoring and combating cyber-attacks and cybercrime at the state level - it is stated in the Strategy.

CIRT is a central point for coordination of prevention and protection against computer security incidents on the Internet and other information systems security risk for Montenegro. In order to better and more efficient way to respond to the incident, it is necessary to provide better collaboration and seamless information exchange between key institutions in the field of cyber security. This primarily refers to the cooperation of key state institutions with key institutions in the private sector (internet service providers, agent for .me domain, mobile operators, banking, electricity, post office ...).

Given that cyber-attacks know no boundaries, and that many of these attacks are coming from other countries, it is necessary to be added, to establish and maintain cooperation with relevant international institutions and national CIRT teams from other countries.

The formation of the National Council for cyber security, gets an umbrella organization in the country, which will advise the Government of Montenegro on all important issues related to cyber security. The Council will propose measures for harmonization of the legal and administrative framework in order to effectively fight against cybercrime. Council members are representatives of key institutions that are recognized in the fight against cybercrime - according to a strategy.

References

[1] Faculty of Political Science, [Online]. Available: http://www.fpn.co.me/. [Accessed 23 Jun 2014].

[2] Faculty of Electrical Engineering, [Online]. Available: http://www.etf.ucg.ac.me//. [Accessed 23 Jun 2014].

[3] Faculty of science, [Online]. Available: http://www.pmf.ac.me/. [Accessed 23 Jun 2014].

[4] Ministry of Information society and telecommunications of Montenegro, »Cyber Security Strategy for Montenegro 2013-2017«. 2013.