Cyber Security in Montenegro: Practice, Frameworks, and Challenges

Ramo Šendelj, *University of Donja Gorica, Montenegro, ramo.sendelj@gmail.com*
Flavio Lombardi, *Roma Tre University, Italy, lombardi@mat.uniroma3.it*
Ivana Ognjanović, *University Mediterranean, ivana.ognjanovic@unimediteran.net*
Stefano Guarino, *Roma Tre University, Italy, guarino@mat.uniroma3.it*

Abstract

The Internet allows users to gather, store, process, and transfer vast amounts of data, including proprietary and sensitive business, transactional, and personal data. Over the last forty years, and especially since the year 2000, governments and businesses have embraced the Internet, and ICT's potential to generate income and employment, provide access to business and information, enable e-learning, and facilitate government activities. Nowadays, Cyber-security is therefore a priority at national and international level: cyber-threats evolve as rapidly as the Internet expands, and the associated risks are becoming increasingly global. To guarantee protection against such threats, any country needs to put in practice proper mechanisms to make users at any level, from children to professionals, aware of the risks, and to improve their security practices on an ongoing basis. In this paper, we exhibit an accurate analysis of the current state of Montenegro's cyber security practice, performed within the EU TEMPUS project 'Enhancement of Cyber Educational System in Montenegro (ECESM)'. Based on a three-dimensional model, which distinguishes National, Governmental, and International aspects, we review cyber-security in Montenegro with respect to EU standards, highlighting open challenges and possible corrective measures and actions. While this paper is intended to also contribute to the cyber-security literature on governance issues and national security strategies, it only reflects research conducted by the authors, which does not necessarily correspond to the official view of the respective institutions.

1. Introduction

Information and communications technologies (ICT) have become indispensable to the modern lifestyle. We depend on information and communications infrastructure in governing our societies, conducting business, and exercising our rights and freedoms as citizens. In the same way, nations have become dependent on their information and communications infrastructure, and threats against its availability, integrity and confidentiality can affect the very functioning of our societies [6]. Every country needs to protect its own national IT infrastructure, as well as cyber-space which is covered by the national domain. The security of a nation's online environment is dependent on a number of stakeholders with differing needs and roles. From the user of public communications services, to the Internet Service Provider supplying the infrastructure and handling everyday functioning of services, to the institutions ensuring a nation's internal and external security interests – every entity involved in the information system affects the level of resistance of the national information infrastructure to cyber-threats. Successful national cyber-security strategies must take into consideration all the concerned stakeholders, the need for their awareness of their responsibilities, and the need to provide them with the necessary means to carry out their tasks. Also, national cyber-security cannot be viewed as merely a sectorial responsibility: it requires a coordinated effort of all stakeholders [7]. Therefore, collaboration is a common thread that runs through most of the currently available national strategies and policies.

In this paper, in light of Montenegro's recent developments in the cyber-security field, we analyze the current state of cyber security practice in Montenegro using a three-dimensional model [1,2], which distinguish National, Governmental, and International aspects. This paper also aims to contribute to the cyber-security literature on governance issues, as well as to national security preparations. The remainder of the paper is organized as follows. Section 2 recalls the main principles of cyber-security, which allow to identify the scope and methodology of our study. Section 3 presents our findings regarding the current state of cyber-security related activities in Montenegro, placing special focus on the national strategies. In Section 4, we identify the main open issues and provide recommendations on how Montenegro's practices should be improved to address them. Finally, Section 5 concludes the paper.

2. Principles of cyber security

In the literature, different methodological approaches have been proposed to properly analyze national cyber security frameworks (*e.g.*, Macro Analysis Model [1], BASE [3]). However, any approach to assess a country's National Cyber Security (NCS) strategy needs to take into consideration three main dimensions of activities: National, Governmental, and International [2].

National Dimension. As regards the National dimension of activity, engagement with security contractors and critical infrastructure companies has always been considered critical for national security [10]. The steady expansion of the number of actors relevant to national cyber-security within any particular nation pushed some governments to decide to make their overall strategy ‘comprehensive’, including the entire society, or the Whole of Nation. A Whole of Nation approach tries to overcome the limitations of simply having special legally-defined relationships with a small number of specific security contractors. While a similar approach presents many advantages, it may fail to guarantee the adequate level of cooperation among (possibly a wide range of) non-state actors (*i.e.,* companies, research establishments and civil society), as well as between private institutions and the government. A fundamental measure of the quality of a NSC strategy is therefore to which extent it succeeds in encouraging collaboration on cyber security issues [9].

Even within the government itself, it is not unusual for up to a dozen different departments and agencies to be given responsibilities for national cyber-security in various forms. For instance, military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, telecommunications, and other governmental bodies are typically involved in the NSC strategy [9]. A major challenge for all NCS strategies, and another parameter to assess their effectiveness, is therefore the degree of coordination between these governmental actors [11].

Governmental Dimension. Many governments are building capabilities to wage cyber-war: NATO reports confirm that up to 120 countries are developing a military cyber-force [15]. These capabilities can be interpreted as simply one more tool of warfare, which is expected to be used only within clearly defined tactical military missions (for instance, for shutting down an air-defense system). Military cyber-activities encompass enabling four different tasks: (i) protection of the defense networks, (ii) Network Centric Warfare (NCW), (iii) battlefield or tactical cyber warfare, and (iv) strategic cyber warfare [11]. Activities and obtained results in these kinds of tasks have to be measured and evaluated, in order to show evidence of increased cyber-protection. In addition to military issues, governments are facing many other challenges related to cyber-security, such as: counter cyber-crime, intelligence and counter-intelligence, critical infrastructure protection, national crisis management, cyber-diplomacy, etc.

Cyber-crime includes a wide swath of activities that directly impact both individual citizens (*e.g.*, identity theft) and corporations (*e.g.*, theft of intellectual property). However, what is probably most significant for national security is the logistical support that cyber-crime can guarantee to anyone interested in conducting attacks to national security: cyber-activities can in fact be used to facilitate and/or maximize the effects of military/terroristic operations. Furthermore, cyber-terrorism itself represents a serious threat for the future: there has recently been a rising number of criminal acts, including attempts at mass disruption of communications, conducted using digital means [7]. Efforts and obtained results in these kinds of activities have to be measured and evaluated in order to show evidence of increased cyber-security activity against cyber-crime.

Distinguishing cyber-espionage from cyber-crime and military cyber-activities is controversial. In fact, both missions rely on similar vectors of attack and similar technology. In practice, however, serious espionage cases (regarding intellectual property as well as state secrets) represent a class of attacks on their own. Other than protecting confidential data, when dealing with cyber-espionage it is particularly important (and difficult) to ascertain the identity of the perpetrator, *i.e.,* if the attacker is a state or a criminal group, and, in the latter case, if it operates on behalf of a government or on its own. Cyber-espionage activities and their rate of success need to be monitored to assess the quality of a NCS strategy.

Critical Infrastructure Protection (CIP) has become the catch-all term that seeks to involve the providers of essential services of a country within a national security framework. As most of the service providers (e.g.public utilities, finance or telecommunications) are in the private sector, it is necessary to extend some sort of governmental support to help protecting them and the essential services they provide from modern threats. Today the majority of all CIP activity is directly connected to cyber-acts, usually cyber-crime and cyber-espionage. In this context, the National Crisis Management must be extended by an additional cyber-component. CIP-related activities are among the main aspects of a NCS strategy, and their effectiveness requires an accurate evaluation.

‘Cyber-Diplomacy’ concerns ‘how diplomacy is adapting to the new global information order’. Within this context, the activities related to the fulfillment of aims such as ‘norms and standards for cyber-behavior’ (discussed primarily within the UN), and towards promoting ‘confidence building measures between nations in cyber-space’ need to be measured and evaluated. Internet governance, a largely multilateral (or even multi-stakeholder) activity, is much more difficult to evaluate per single Nation.

International Dimension. The very basis of the Internet, not to mention the myriad companies and organizations that effectively constitute the Internet, is thoroughly globalized. It is therefore clear why virtually no NCS document can ignore the international dimension. For any nation state or interest group, advancing its interests requires collaboration with a wide range of international partners. This applies at any level: from internationally binding treaties (*e.g.*, the Council of Europe Cyber-crime Convention), to politically binding agreements (*e.g.*, regarding Confidence Building Measures in Cyberspace), to non-governmental agreements between technical certification bodies (*e.g.*, membership of FIRST and similar bodies). Since it is often necessary to work with international non-state actors, most collaborations usually occur outside the range of a specific national government. Therefore, the emphasis must be on evaluating the reliability of all relationships with relevant actors within specific systems (in particular, but not limited to the field of ‘internet governance’).

3. Cyber security framework in Montenegro

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 need more flexible and dynamic strategies concerning cyber-security. The key document that has been adopted by the Government on September the 12th 2013 is the “National Cyber-Security Strategy for Montenegro 2013-2017” [4], together with the proposed action plan for the implementation of the strategy from 2013 to 2015.

The Cyber-Security Strategy for Montenegro contains seven key areas:

1. Definition of institutional and organizational structures in the field of cyber-security in the country;
2. Protection of critical information structures in Montenegro;
3. Reinforcement of capacities of state law enforcement authorities;
4. Incident Response;
5. Clarification of the role of Ministry of Defense and Military of Montenegro in cyber-space;
6. Development of public-private partnerships;
7. Improvement of public awareness and protection on the Internet.

The Strategy further defines the following concrete activities, which should be implemented in the upcoming period by key decision makers: (i) Set the vision, scope, aims and priorities; (ii) Follow risk assessments on the national level; (iii) Take into consideration existing policies, regulations and capacities; (iv) Develop a clear managing structure; (v) Identify and include interested parties; (vi) Set confidential mechanisms for information exchange; (vii) Develop cyber-safety plans for unforeseen emergencies; (viii) Organize cyber-security exercises; (ix) Set up basic security demands; (x) Develop mechanisms of incident reporting; (xi) Increase awareness of citizens on this issue; (xii) Nourish cycle of research and development; (xiii) Strengthen capacities through trainings and advancement programs; (xiv) Set up incident response capacity; (xv) Respond to cyber-crime; (xvi) Engage in international cooperation; (xvii) Set up public-private partnerships; (xviii) Balance between security and privacy protection; (xix) Conduct evaluation; (xx) Align National Strategy on cyber-safety.

National Organizations in Montenegro. Within the public administration, Montenegro needs to establish a precise organizational hierarchy able to ensure the appropriate security in information management, in the most efficient and (long-term) sustainable way. In Montenegro, the key institutions essential to the field of cyber-security are:

• ***Ministry for Information Society and Telecommunications (National CIRT)*** - The national CIRT represents a central body for coordination and exchange of data, defense from cyber-attacks, and recovery from cyber security incidents in Montenegro. The CIRT is appointed to handling information security incidents, whenever at least one of the parties involved in the incident is Montenegrin (*i.e.,* if it belongs to the “.me” domain, or if it is within the Montenegrin IP address space). 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.

• ***Ministry of Defense*** – The Ministry of Defense is actively involved in cyber-security. Its key activities in the field: defining the role of the military force in the cyber-space of Montenegro; improving the capacity of the Military of Montenegro in the field of cyber-defense; establishment of cooperation in this field with international partners.

• ***Ministry of the Interior*** – The main duty of the Ministry of the Interior for what concerns cyber-security is to enforce specialized 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 any illegal act that can be done with the help of a computer.

• ***Ministry of Justice***

• ***Military of Montenegro***

• ***Universities in Montenegro*** – The scope of Montenegrin universities and other educational institutions is to improve the skills of the new generations, to produce a well-prepared future work force. New programs about information security should be continuously introduced at all educational levels, in order to raise the awareness of end-users of the Internet and make them capable of using advanced information systems. However, only a limited number of cyber-security courses are established in total in the three universities in Montenegro, highlighting a lack of educational programs in the area.

Cyber-security standards and frameworks. Since 2005, Montenegro started creating its institutional and legal framework, which prevents any kind of accidental or intentional breach or incapacitating of informational systems, through reform of its criminal legislation. Adoption of new and improvement of existing primary and secondary legislation, represents a key element for existence of information security in Montenegro. An adequate legal framework represents a link between legislation and information technology, which should contribute to successfully resolving cases in the field of cyber-crime, and to properly sanctioning the perpetrators.

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

1. Law on Ratification of Convention on Cybercrime [14];
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. National Cyber Security Strategy for Montenegro 2013-2017 [4];
11. Study with defined responsibilities of state authorities in fight against cyber-crime 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);
15. Regulation on method of conducting and content of internal control over implementation of measures to protect classified information (28th July 2010).

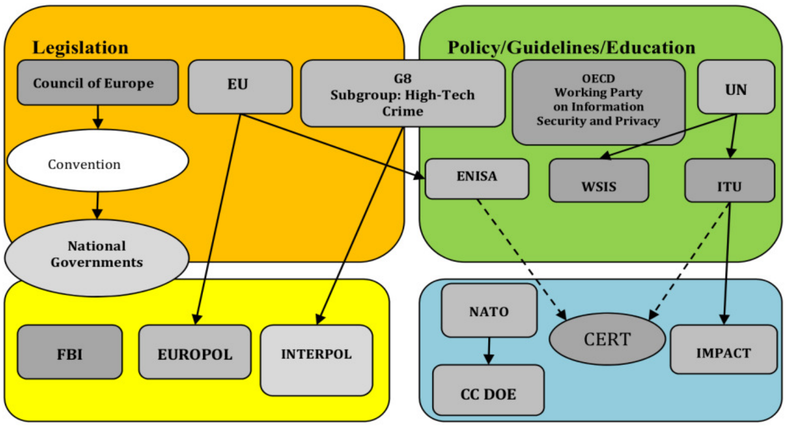

Figure 1: Key Intergovernmental Institutions [5]

International standards and frameworks. The issues of cyber-security vulnerabilities, national security, public safety, economic prosperity and critical infrastructures were discussed on the Explanatory session between EU and Montenegro (December 2012) during the Screening chapter 10 – "Information society" [13]. The EU has highlighted the necessity for Montenegro to begin with coordinated national initiatives focused on cyber-security awareness, education, trainings, and professional development.

Strategic priorities are thus defined in accordance with EU standards and good practices, summarized in Figure 1. All key factors can be seen in the figure, with presented inter-connections and joint actions. The aforementioned organizational structure with established frameworks and standards in Montenegro should be cross matched with the model presented in Figure 1. Major findings are presented in the following sections.

4. Findings and Recommendations

Keeping in mind that the strategic goal of Montenegro is to build an integrated, functional, secure and efficient cyber-space, in accordance with international standards and principles, Montenegro has adopted its National Cyber Security Strategy, in July 2013, for the period 2013-2017. The Strategy clearly defines aims and priorities, and represents vision of Montenegro in terms of cyber-security and its granting. Based on this strategy, Montenegro has adopted annual Action Plans. Formally, from the perspective of frameworks and regulations, Montenegro seems to have already reached the most common standards in place. This is probably due to the fact that similar aspects are among the easiest one to adopt by simply taking inspiration from EU countries. However, several aspects of cyber-security planning still need to be properly addressed. Furthermore, it is very important to assess to which extent strategies and plans have been put in practice. In the remainder of this section, we will recap the main open issues we identified.

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: (i) a novel legal framework, including cyber-crimes under all possible forms; and (ii) the 'National Cyber-Security Strategy for Montenegro 2013-2017", that is, a plan for National cyber-defence in the upcoming years. 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 cyber-crime. To this end, we identify the following steps that need to be urgently addressed:

- Clarify the role of the military force in preserving (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.
- Fill the lack of a National Cyber Security Council with its functions: (a) coordination of information security in Montenegro; (b) review of the legislative framework for the development of operational cyber-security; (c) identification of critical information infrastructure.
- 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, 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 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.
- Address the absence of procedures about keeping records on incident situations in Montenegrin cyber-space.
- Double-check the legal framework against EU standards: even if the legal framework seems well structured and elaborated, 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.

Cyber security Education in Montenegro. Many universities in the EU are in the process of setting up a cyber-security curriculum. Often these curricula are interdisciplinary, as is the case in Montenegro. Indeed, this is especially true for smal 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 came to the following to-do list:

- Raise awareness about cyber-security over Montenegrin population in general. The purpose should be to educate all population about possible threats over the Internet, and make them familiar with basic rules about safe surfing, and securely using online accounts and services.
- Establish sustainable strategies for training a skilled workforce in specific fields and areas of action, such as: law enforcement, training judiciary, ICT sectors, etc. The aim is to ensure that law enforcement agencies have the capabilities and competencies necessary to investigate cyber-crime, to provide electronic evidence, to conduct computer forensic analysis in criminal proceedings, to help other bodies and contribute to network security. On the other hand, ICT professionals should be able to use modern technologies in order to design security systems and respond to different kinds of identified attacks [12].
- In order to ensure sustainable education in cyber-security, core elements of the formal educational system in cyber-security (graduate and post-graduate studies) should be identified, including both formal and informal education. In accordance with the above priorities, its core elements should include literacy of cyber-security at lowest levels in the educational system, and specialized higher education such as post-graduate and master studies. All other elements of the educational system may be established later in full coherence with those core elements.

- Establish collaborations and cooperation at regional, institutional, national and international level, aimed at exchanging experience and knowledge, and enhancing joint forces in cyber-war. It can be realized by establishing joint regional centers for cyber-security (such as regional CERT, regional joint studies in cyber-security, etc.) and/or joint participation in different project funded by EU and other international sources.
- Integrate training on cyber-crime in regular programs at private and public institutions/agencies.
- Create Research and Development (R&D) environments in the field of cyber-security. R&D activities are in fact essential in order to prepare own national forces to face a challenge on dynamic and constantly evolving and growing cyber-space. To this end, PhD studies should be established with simultaneous preparation at institutional and individual (already proven researchers with expressed willingness and readiness for R&D in cyber-security field) levels to lead those activities at national and/or regional level.

5. Conclusions

Since nations have become increasingly dependent on their information and communications infrastructure availability, integrity and confidentiality, cyber-security issues are extremely relevant at national and international level to securely governing societies, conducting business, and exercising rights and freedoms as citizens. In this paper, we surveyed the main principles of cyber-security, and described the fundamental characteristics that determine the quality of national cyber-security strategies and frameworks. We later focused on Montenegro, to assess its compliance to EU cyber-security standards, and to identify possible directions to improve its cyber-security practices. We underlined how Montenegro adopted a clear National Cyber Security Strategy, containing all main relevant key areas, and defining aims and priorities, representing the vision of Montenegro in terms of cyber-security and its granting. Annual Action Plans seem to have allowed Montenegro to reach the most common standards in place, by taking inspiration from EU countries. However, much still needs to be done: we highlighted both deficiencies in the national framework and structure, and issues concerning awareness and education. The road to fill the gap with EU countries is long, but Montenegro took the right path, and we hope that this paper can help clarifying the route.

Acknowledgements. Research presented in this paper is conducted within the TEMPUS project ‘Enhancement of Cyber Educational System in Montenegro (ECESM)’, project no. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

6. References

1. H. Şentürk, C.Z. Çil, and Ş. Sağıroğlu, “*A Proposal for a Cyber Security Macro Analysis Model and Analysis of Turkey*”, In Proc. of the 5th International Conference on Information Security and Cryptology, 15-17 May 2012, Ankara, Turkey.
2. U. Gori, “*Modelling Cyber Security: Approaches, Methodology, Strategies*”, NATO Science for Peace and Security Series - E: Human and Societal Dynamics, 2009
3. G. Braunton, “*B.A.S.E. - A Security Assessment Methodology*”, SANS Institute 2005
4. Government of Montenegro, *National Cyber Security for Montenegro 2013-2017*
5. Tempus project-ECESM, *Report-DEV 1.1 Existing EU practices for cyber security,* website: http://ecesm.net/publications-0
6. P. G. Neumann.”*Risks to the public*”. SIGSOFT Softw. Eng. Notes 37, 4 (July 2012), 20-29.
7. M. D. el Kettani and T. Debbagh, ” *NCSec: a national cyber security referential for the development of a code of practice in national cyber security management*”. In Proc. of the 2nd Int. conference on Theory and practice of electronic governance, 2008
8. D. Klaper and E. Hovy. “*A taxonomy and a knowledge portal for cybersecurity*”. In Proc. of the 15th Annual International Conference on Digital Government Research (dg.o '14). 2014, ACM, New York, USA
9. J. Harašta, "*Cyber Security in Young Democracies*." Jurisprudencija 20 (4), pp.1457-1472, 2013
10. M. Suter, “*A Generic National Framework For Critical Information Infrastructure Protection (CIIP)*”, Center for Security Studies, ETH Zurich, 2007
11. E. Yuan, N. Esfahani, and S. Malek. “*A Systematic Survey of Self-Protecting Software Systems*”. ACM Trans. Auton. Adapt. Syst. 8 (4), No. 17, 2014
12. M. Prandini and M. Ramilli, “*Security considerations about the adoption of web 2.0 technologies in sensitive e-government processes*”. In Proc. of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV '11), Elsa Estevez and Marijn Janssen (Eds.). ACM, New York, NY, USA, 285-288.
13. EU, *Screening report Montenegro Chapter 10 Information society and media* http://ec.europa.eu/enlargement/pdf/montenegro/screening_reports/screening_report_montenegro_ch10.pdf
14. M.A. Vatis, “*The Council of Europe Convention on Cybercrime*”, https://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf
15. NATO Emerging Security Challenges Division, *The World in 2020- Can NATO Protect Us? The Challenges to Critical Infrastructure*, Conference Report, 2012, Brussels