CIIP Related Activities in Bosnia and Herzegovina

Haris Hamidović

Abstract—**Critical Information Infrastructure Protections (CIIP) is one of the key priorities of the European Union. High dependence on critical information infrastructure, their cross-border interconnection and interdependencies with other infrastructures, as well as the vulnerabilities and threats they are exposed to increase need to address issues of their security and resilience in a systematic way.**

There are numerous new EU initiatives in this area such as the adoption of regulations that regulate the issue of security and integrity of public communications networks, the measures aimed at addressing the issues of security of European operators of critical infrastructure, redefining the role of the European Agency for Network and Information Security related to CIIP, harmonization of the criminal legislation regarding cyber crime, funding for relevant research and development in the EU, etc.

CIIP is a global issue that impacts developed and developing countries alike. Developing countries present a challenge that cannot be ignored without risk to global cyber security.

The main objective of this paper is to presents the results of initial assessment of national preparedness of Bosnia and Herzegovina for the risk management of critical information infrastructure, based on ENISA methodology, and to provide an overview to the law of information security in Bosnia and Herzegovina.

Index Terms—**BiH, CIIP, CII, cyber security, ENISA, NRM.**

I. Introduction

The Council of Ministers of Bosnia and Herzegovina (BiH) adopted in 2004. the Policy of Information Society Development in BiH as the framework and basic document, in accordance with which the future legislation, acts and other regulations will be passed in the process of building and development of information society, and also upon which the future decision will be taken on the development directions, action plans and priorities at the level of BiH and its entities. This Policy has expressed the ambitious goal for building of BiH as a modern and prosperous society. The vision's realizations of such a society is the task of the highest level of complexity. It requires, above all, a consensus, as well as coordinated efforts and support at the state level of all the relevant political factors.

The Policy of Information Society Development in BiH stated that the network and information security are important and necessary for the functioning of the information society. However, current organizational, personnel, technical, operational and other arrangements have not resulted in achieving a desirable environment that is essential for the development of a secure information society in BiH. There are evident multiple difficulties and obstacles, which on the other side causes destabilization of developmental perspective. BiH is in a very specific political, security, economic, financial and other circumstances because of various difficulties and obstructions, particularly when it comes to the adoption of laws at the state level.

Manuscript received February 28, 2013; revised June 15, 2013.

Haris Hamidović is with the Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina (e-mail: haris.hamidovic@eki.ba).

II. Critical Information Infrastructure Protection

Critical Information Infrastructure Protections (CIIP) is one of the key priorities of the European Union (EU). High dependence on Critical Information Infrastructure (CII), their cross-border interconnection and interdependencies with other infrastructures, as well as the vulnerabilities and threats they are exposed to increase need to address issues of their security and resilience in a systematic way.

There are numerous new EU initiatives in this area such as the adoption of regulations that regulate the issue of security and integrity of public communications networks, the measures aimed at addressing the issues of security of European operators of critical infrastructure, redefining the role of the European Agency for Network and Information Security related to CIIP, harmonization of the criminal legislation regarding cyber crime, funding for relevant research and development in the EU, etc.

The importance of the protection of the risk to CII within EU countries has been emphasized by the Commission of the European Communities in its communication: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM (2009) 149).

III. National Risk Management Preparedness

National Risk Management (NRM) preparedness is primarily the concern of national governments and national security institutions. However, all organizations, whether part of national government or of an individual sector, must attach equal importance to the implementation of risk management within their own organization. [1]

In 2011, European Network and Information Security Agency (ENISA) presented the framework for the governance of NRM in relation to a country's CII.

Having considered the congruency of information security risk management and NRM, ENISA ad hoc Working Group on National Risk Management Preparedness concluded that there are three essential components to the governance of information security risk management in the context of EU member states. These three elements may be described as follows:

1) The establishment of a policy framework to encourage the use of risk management within CII stakeholder

organizations in both public and private sectors within EU countries.

2) The investment by EU countries in measures to support individual CII stakeholder organizations in their implementation of appropriate risk management activities.
3) The ability of EU countries to monitor and review current NRM implementation levels and adapt national activities accordingly.

IV. Initial Assessment of BiH's NRM Preparedness

At the level of Bosnia and Herzegovina and its entities there is still no strategy for protecting CII or government body with responsibility for this area. Specific cyber security initiatives exist at the state level, but it could be characterized as fragmented and uncoordinated with each other.

Fig. 1 shows the results of initial assessment of national preparedness of Bosnia and Herzegovina for the risk management of CII, based on the ENISA methodology. [1] The data was collected during 2012. through interviews and on-line questionnaires with 37 CIOs and IT auditors in BiH's organizations critical infrastructure industries (finance, energy, health ...) and audit companies. Fig. 1 indicates average respondents' assessment of capability maturity (using the COBIT capability maturity measurement scale from non-existent (0) to optimized (5)) in each of the 12 NRM activities:

A1: Set the vision;
A2: Establish NRM organization;
A3. Support and regulate;
A4: Promote awareness;
A5. Provide necessary information;
A6: Promote standards;
A7. Foster collaboration;
A8. Monitor effectiveness;
A9. Analyze errors and incidents;
A10. Review effectiveness;
A11: Report on NRM process maturity; and
A12: Suggest improvements.

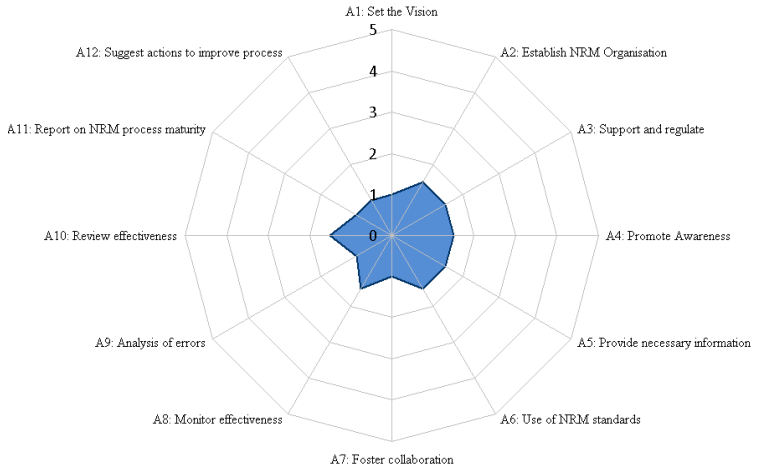

Fig. 1. Initial assessment of national preparedness of BiH for the risk management of CII

Fig. 2 present the results of initial assessment of national preparedness of Bosnia and Herzegovina in relation to the results of the preliminary assessment done in 4 EU Member States.

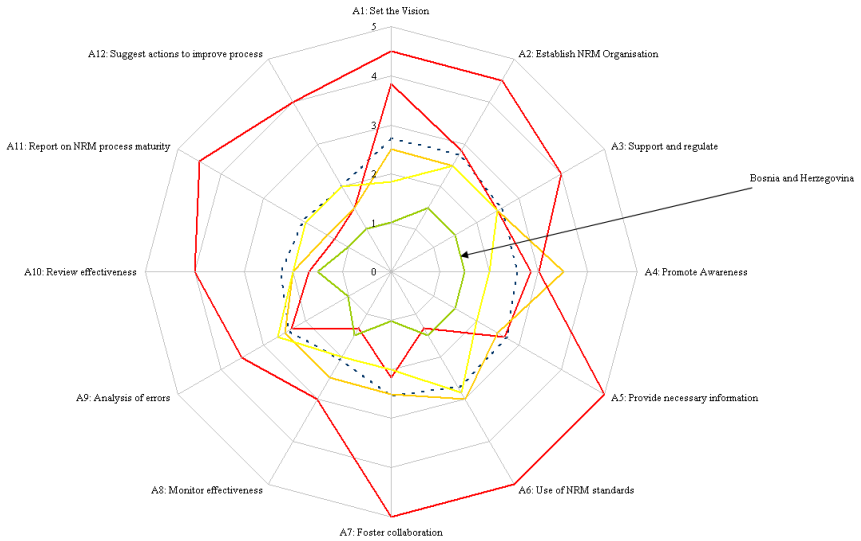

Fig. 2. Comparison of the level of national preparedness of BiH and the EU countries

The initial assessment indicates that BiH's readiness for risk management of CII is behind EU countries. The big

problem of the ICT sector in BiH is the lack of central ministries (departments, agencies) at the state level, whose primary task would be to develop the capacity to manage the risk of critical national information infrastructure.

Many institutions in BiH are dealing with ICT, but few of them do it in a systematic way. This segment requires a significant investment, but of that will be depended not only advances of ICT and other industrial sectors, but also the comprehensive development of BiH. [2]

V. CIIP Related Activities in BiH

The legislator in BiH essentially takes a two-pronged approach to addressing the challenges posed by the extensive use of electronic information, and the potential damages that can arise when security is breached and information is compromised:

1) First, criminal law declares illegal certain conduct that breaches the security of one's data, and provides punishment for those who engage in such conduct.
2) Second, some law and regulation imposes on those businesses that possess data an obligation to protect that data and the corresponding information systems in order to protect the various stakeholders.

Bosnia and Herzegovina has ratified and signed the Council of Europe Convention on Cybercrime, and modified existing entities criminal laws, but still not criminal law at the state level, to better fit computer crimes.

The Preamble to the Council of Europe Convention on Cybercrime makes note of [3]:

1) the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime;
2) the profound changes brought about by the digitalization, convergence and continuing globalization of computer networks;
3) the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; and
4) the need to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data.

Harmonization of BiH and European criminal legislation in the area of cyber crime can contribute to CIIP protection, but considering complexity of investigating crime in the ICT environment [4] and the fact that BiH does not have sufficient and appropriate legal, human resources and technical capacity to effectively combat this type of crime [5] this may have limited deterrent effect aimed at commission of such criminal acts.

Inadequate legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information and systems. [6]

Of the entire critical infrastructure sector in Bosnia and Herzegovina, it is only in the banking sector of the Federation BiH which is appropriately regulated governance of information technology. Specifically, the Banking Agency of the Federation of Bosnia and Herzegovina adopted in early 2012 the Decision which sets minimum standards and criteria that banks are required to provide and implement in the process of managing information systems. By this Decision Banks in the Federation BiH are required to establish, implement, monitor, maintain, regularly review and improve the process of managing information systems in order to reduce risk exposure, ensuring confidentiality, integrity and availability of information and overall information system is in accordance with size, complexity and scope of the bank and complexity of information systems. [7]

Data protection legislation in BiH, as well as in many other countries, governs the treatment of certain types of information, broadly defined as information about individuals, described as "personal data" in the legislation. Bosnia and Herzegovina's data protection law is based on the European Union Data Protection Directive. This law requires that the data controller implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures need to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Special categories of personal data include all personal data that, among other things, reveal state of health and genetic code. The data controller must take additional technical and organizational measures in processing the special categories of personal data, which especially should take into account health sector organizations in BiH. [8] Unauthorized entry into another's protected computer database of personal data, constitute a criminal offense for which are envisaged penalties up to one year in prison. [9] Computer database of personal data must be protected. If, however, the data controller has not taken appropriate technical and organizational measures to protect personal data, data controller can be punished by a fine of up to 50,000 Euros. [10]

VI. Conclusion

Increasingly, national security and the physical, economic, and institutional infrastructures at the core of modern life are dependent upon information infrastructure.

The risks and threats to information systems are increasing faster than countermeasures can be developed. An interconnected global network demands that cyber security be approached from an international perspective.

Cyber security is a global issue that impacts developed and developing countries alike. Because it requires a global effort it cannot be achieved by one or a handful of nations. It requires the involvement of all users of information and communication technologies, including citizens, governments, industry, and organizations. To make whole cyberspace more secure industrialized nations must provide technical assistance to developing nations to help them secure their infrastructure.

An effective response to threats to national critical information infrastructure requires a multidisciplinary

approach (technical, criminal legislation, national security, economic ...).

The initial assessment of national preparedness of Bosnia and Herzegovina for the risk management of critical information infrastructure indicates that BiH's readiness for risk management of CII is behind EU countries. Since Bosnia and Herzegovina currently has no capacity to fully develop by itself security standards for critical infrastructure systems it should follow the practice of developed countries.

It should be borne in mind that only the formal approval of CIIP protection strategy, in order to meet form and formal requirements that are placed for Bosnia and Herzegovina within the Euro-Atlantic integration is not sufficient. What is needed is to build such a framework - a system of protection that will provide:

1) Continuity of the functioning of the CIIP system;
2) Increased efficiency of CIIP system
3) Continuity of increasing the effectiveness of the CIIP system.

REFERENCES

[1] *ENISA ad hoc Working Group on National Risk Management Preparedness - Consolidated Report, Version: 1.0,* ENISA, ExecIA LLP, 2011.

[2] *Mid-term Development Strategy of Bosnia & Herzegovina 2004-2007,* The Directorate for Economic Planning BiH (DEP), 2004.

[3] *Convention on Cybercrime – Budapest, 23.XI.2001 (ETS No. 185),* The Council of Europe, 2001.

[4] H. Hamidović, "Main Characteristics of Digital Evidence," in *Proc. of the 5th International scientific and technical conference "Forensic Investigations"*, Oct. 14th - 15th, 2011, the International Association of Criminalists - IAK, Banja Luka, pp. 362-372, vol. 4, issue I.

[5] The Prosecutor's Office of Bosnia and Herzegovina, *Annual Report of the Prosecutor's Office of BiH,* 2011 (in Bosnian) (Tužilaštvo Bosne i Hercegovine, *Informacija o radu za 2010*., 2011)

[6] *Cyber Crime…and Punishment? Archaic Laws Threaten Global Information,* McConnell International LLC, 2000.

[7] The Banking Agency of the Federation of Bosnia and Herzegovina (FBA), *The Decision on Minimum Standards for Governance of Information Systems in the Banks* ("Official Gazette of FBiH", No. 1/12), 2012.

[8] H. Hamidovic and J. Kabil, "An Introduction to Information Security Management in Health Care Organizations," *ISACA Journal*, vol. 5, Information Systems Audit and Control Association, 2011.

[9] The National Assembly of the Republic of Srpska, *Criminal Code Of the Republika Srpska* (Official Gazette of RS, no. 49/03), 2003.

[10] The Parliamentary Assembly of Bosnia and Herzegovina, *The Law on Personal Data Protection*, Official Gazette of Bosnia and Herzegovina, no. 49/06, 2006.

Hamidović Haris received the B.S. degree in electrical engineering from University of Tuzla, Tuzla, Bosnia and Herzegovina in 1997, the M.S. degree in information technology from University Dzemal Bijedic of Mostar, Mostar, Bosnia and Herzegovina in 2007. He is a doctoral candidate in critical information infrastructure protection at the University Dzemal Bijedic of Mostar, Mostar, Bosnia and Herzegovina.

He is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the North American Treaty Organization (NATO)-led Stabilization Force (SFOR) in Bosnia and Herzegovina. He is the author of five books and more than 60 articles for business and IT-related publications. Hamidovic is a certified IT expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina and the Federal Ministry of Physical Planning of Bosnia and Herzegovina.

Mr. Hamidovic is a member of the Institute of Internal Auditors (IIA) and the Information Systems Audit and Control Association (ISACA).