CASE STUDY

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Beyond Physical Threats: Cyber-attacks on Critical Infrastructure as a Challenge of Changing Security Environment – Overview of Cyber-security legislation and implementation in SEE Countries

Ivana Cesarec, Croatian Ministry of Interior, Civil Protection Directorate

Address for correspondence: Ivana Cesarec, Croatian Ministry of Interior, Civil Protection Directorate, e-mail: ivevg1@gmail.com

Abstract

States, organizations and individuals are becoming targets of both individual and state-sponsored cyber-attacks, by those who recognize the impact of disrupting security systems and effect to people and governments. Wide range of critical infrastructure sectors are reliant on industrial control systems for monitoring processes and controlling physical devices and for that reason, physical connected devices that support industrial processes are becoming more vulnerable. Not all critical infrastructure operators in all sectors are adequately prepared to manage protection (and raise resilience) effectively across both cyber and physical environments. Additionally there are few challenges in implementation of protection measures, such as lack of collaboration between private and public sector and low levels of awareness on existence of national key legislation.

From supranational aspect, in relation to this papers topic, the European Union has took first concrete step in defense to cyber threats in 2016 with „Directive on security of network and information systems“ (NIS Directive) by prescribing Member States to adopt more rigid cyber-security standards. The aim of directive is to improve the deterrent and increase the EU's defenses and reactions to cyber attacks by expanding the cyber security capacity, increasing collaboration at an EU level and introducing measures to prevent risk and handle cyber incidents. Yet, not all Member States share the same capacities for achieving the highest level of cyber-security. They need to continuously work on enhancing the capability of defense against cyber threats as increased risk to state institutions information and communication systems but also the critical infrastructure objects. In Southeast Europe there are few additional challenges – some countries even don't have designated critical infrastructures and they are only perceived through physical prism; non-EU countries are not obligated to follow requirements of European Union and its legislation, and there are interdependencies and transboundary cross-sector effects that needs to be taken in consideration. Critical infrastructure Protection is the primary area of action, and for some of SEE countries (like the Republic of Croatia) the implementation of cyber security provisions just complements comprehensive activities which are focused on physical protection.

This paper will analyze few segments of how SEE countries cope with new security challenges and on which level are they prepared for cyber-attacks and threats: 1. Which security mechanisms they use; 2. The existing legislation (Acts, Strategies, Plan of Action, etc.) related to cyber threats in correlation with strategic critical infrastructure protection documents. Analysis will have two perspectives: from EU member states and from non-EU member states point of view. The aim of research is to have an overall picture of efforts in region regarding cyber-security as possibility for improvement thorough cooperation, organizational measures, etc. providing also some recommendations to reduce the gap in the level of cyber-security development with other regions of EU.

Keywords

Cybersecurity, Legislation, SEE countries, NIS directive, CIP

1. Introduction

The Global Risks Report 2017 of the World Economic Forum rates cyber risks right after the terrorism as the dominant social threat of the twenty-first century. Cyber-security and cyber-space protection is becoming increasingly complex by each day, as a direct consequence of the development of technology, globalization, the emergence of new challenges such as asymmetric threats and other forms of new security threats. Although the use of information and communication technology has a positive impact on the development of the functional capabilities of numerous systems, increasingly interconnected devices and information flows are raising the vulnerability of the objects and other linked critical infrastructures, primarily through the exposure to cyber threats and information and communication infrastructure failures. Systems and infrastructures become very fragile and more prone to risk, which can cause dysfunction but also result in major technological collapse (Mikac, Cesarec and Larkin, 2018: 181). According to researches, attacks on critical information infrastructures are mostly affecting the financial, information and communications technology and energy sectors (Tofan, et.al., 2016:4), which is directly linked to the concept of interdependence that makes infrastructure the most vulnerable, where, for example, "the outage of a hydro or thermal power plant will not only adversely affect the energy sector but also the information, telecommunications, economic, financial and the whole range of services, but the same is equal in the other way" (Matika, 2009: 51).

The goods, products and services in the physical facilities is increasingly being replaced by virtual ones, which, although an asset for community development and a precondition for global collaboration and connectivity, also causes an additional threat of cyber attacks and shifts the focus of national security issues to cyber security. Technology binds, enables work and progresses in development for (critical) infrastructure in all sectors, therefore it is necessary to give attention to infrastructure protection in the cyber dimension as well. It is important to emphasize that the security system includes not only physical protection, but also protection of data and information systems (i.e. electronic services, which are connected to a certain critical infrastructure) and full implementation of adequate information security policies, as well as the protection of the cyber space in which they originate and transmit different types of data. Critical information infrastructure, therefore, is an electronic flow of information, and in this sense cyberspace itself is a critical information infrastructure, which implies the need for a close connection between the concepts of critical infrastructure protection and cyberspace (Perešin and Klaić, 2012: 336).

The Global Cybersecurity Index[1] 2017 presented modeling approach of five strategic pillars on cybersecurity, highlighting legal, technical, organizational, capabilities and cooperation. It also emphasizes that cybersecurity is not only the IT security, it also includes organizational, personal and physical security measures. But what we are witnessing today, business processes often overlook physical security when considering cyber security as main threat. Still, what is virtual takes place through the physical (cameras, sensors, cables) and it is very intertwined. However, although contemporary information systems threats can be classified into characteristic groups of failures, incidents, and attacks, the specificity is that we must clearly distinguish two important categories of information system threats from the traditional understanding: unstructured threats (hackers, individuals) and structured threats (foreign states, terrorists and criminal organizations) (Klaić and Perešin, 2012:2). Referring to the strategic component, especially in the context of security policies that are actually the basis of social action, the role of critical information infrastructure and its impact to CIP policy is extremely significant, which has become evident in the increasing interplay between these two domains. In the beginnings of establishing the regulatory framework in the European Union in the field of critical infrastructures, following a shift in the legislative focus from the threat of terrorism, Directive 2008/114/EC *on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* was adopted, emphasizing two sectors: energy and transport, but also stating that it „...should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector (Council of the European Union, 2008:1). Due to the increasing importance and advancement of technology, the need to further develop the legislative area related to cyberspace has been recognized. One of the most important documents is certainly the NIS Directive (Directive (EU) 2016/1148 *of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*) adopted in 2016, but the EU has been dealing with cyber security issues comprehensively since 2004, starting with founding of ENISA (European Union Agency for Network and Information Security), as a specialized EU agency. In 2009, there was also a *Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* (COM (2009)149), which focuses on prevention and awareness and defines a plan of immediate action to strengthen the security and trust in the information society. It was followed, by a *Joint Communication to the European Parliament, the Council the European Economic and Social Committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* which also emphasizes the need to intensify on-going efforts to strengthen Critical Information Infrastructure Protection. These were initial step towards creating EU Cybersecurity policy, and based on them, and the need to have a common level of security of network and information systems in all Member States, NIS Directive was drafted and entered into force in August 2016. The deadline for national transposition by the EU Member States was 9 May, 2018. Today, the NIS Directive presents main legislation of the Cybersecurity Strategy of the European Union and is extremely significant for the implementation on network and information systems and services which play a vital role in the society. The NIS Directive was adopted to connect the key areas, actors and processes, in order to increase the level of protection and the providing minimum common standards in this field.

Putting in the mutual context the NIS Directive and Directive 2008/114/EC, the NIS Directive arose from the need to complement the existing normative CIP framework, because of the lack of adequate critical infrastructure protection in the information and communication technology sectors. Although, it is important that the NIS directive puts emphasis on information and technology sector (for the raising of the level of security in all sectors dependent on IT), an additional challenge arises in which the critical infrastructure operators are also becoming Operators of critical infrastructures and Operators of Essential Services which results in overlapping or duplicating their obligations (in the allocation of resources, the additional involvement of the staff and experts to increase resilience and the level of protection). It is important for this research to emphasize that the Directive 2008/114/EC is more focused on assets, while the NIS Directive is more focused on services. In that part it is shown aforementioned relationship between the physical and the "virtual" and an indication of the challenge in the interconnection of these two components. In order not to make the analysis of the challenges of changing security environment and the impact on Southeast Europe countries too extensive, the focus of this research will be on four countries with different specificities - two EU Member States and two non-EU countries. In the first group, the Republic of Croatia – as the last Member State to acquire full EU membership in 2013 (although it does not yet have the same capacity as other Member States) had to adapt to the new requirements of Directive 2008/114/EC and the NIS Directive; and Romania which is already a long-standing member of the EU (since 2007) with presumption of success in implementing the provisions of the mentioned Directives. Selected non-EU countries that are part of this analysis are Montenegro, which has the status of candidate for accession since 2006 and North Macedonia since 2005, and must align with the requirements placed on all countries wishing to become part of the community that focuses on setting a high level of security. With those requirements, there is often a lack of awareness of the possibilities and differences that countries have in fulfilling such conditions. Primarily because in the vast majority of SEE countries, the all-hazard approach is based specifically on the physical domain of critical infrastructures, yet the cybersecurity domain cannot be neglected - given its high impact on the security of networks, systems and data that are allowing critical infrastructures to deliver essential services.

2. EU states and non EU-states – understanding the differences in the approaches to CIP and CIIP security policy

The introduction of security measures and standards, both physical and information security, through specific policies in legal entities in different sectors of society should form the basis of a national regulatory framework for information security. Although sectoral approaches are somewhat different, the common threats that arise in their environment and the need to manage risk, imposes a need for a comprehensive approach in critical infrastructure protection.

We can define information infrastructure in general as “a combination of computer and communication systems that serve as the basic infrastructure for public bodies, industry and the economy. Critical infrastructures such as the transportation and distribution of electricity are inevitably dependent on telecommunications, public telephone networks, the Internet, terrestrial and satellite wireless networks and associated computer resources for information, communication and control management” (Brnetić et.al., 2013: 6). Infrastructure objects are also inter-linked in cyberspace, through systems such as Supervisory Control and Data Acquisition Systems - SCADA Systems.

In the context of EU security policy, the NIS Directive brings definition where network and information system means: (a) an electronic communications network; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data or; (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance (The European Parliament And The Council Of The European Union, 2016:13). The definition from Directive 2008/114/EC say that infrastructure is the “asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions“. The fundamental link between these two definitions is the provision of services essential for the maintenance of critical societal and economic activities. For example, energy technologies used before today's extremely advanced technologies, are becoming rapidly more connected (and dependent) to modern, digital technologies and networks. Digitalization makes the energy system better, through new means, such as advanced innovative energy services, yet it also creates significant risk making energy sector more exposed to cyber security incidents.

Due to such inevitable changes, the European Commission is developing measures and mechanisms for its Member States to meet the challenges of today. The basis of these efforts is the establishment of a comprehensive legislative framework based on three documents: the aforementioned “*Cybersecurity Strategy of the European Union: An Open, Safe and*

SecureCyberspace“ (EU Cybersecurity strategy (JOIN (2013)01 final); NIS Directive (the *Directive on Security of Network and Information Systems* (EU) 2016/1148) and the *Joint Communication To The European Parliament And The Council “Resilience, Deterrence and Defense: Building strong cybersecurity for the EU*“ as the Cybersecurity Package (JOIN (2017) 450 final) from September 2017, which also includes the *Cybersecurity Act* which strengthens the EU Agency for cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services and processes. The aforementioned Act provides for a comprehensive set of measures that build on previous actions and fosters mutually reinforcing specific objectives: Increasing capabilities and preparedness of Member States and businesses; Improving cooperation and coordination across Member States and EU institutions, agencies, and bodies; Increasing EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises; Increasing awareness of citizens and businesses on cybersecurity issues; Increasing the overall transparency of cybersecurity assurance of ICT products and services to strengthen trust in the digital single market and in digital innovation; Avoiding fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors. So, the EU Member States have the tools and policies required to address cybersecurity, but it still remains a national priority and responsibility. National cybersecurity strategies are the main documents to set strategic principles, guidelines, and objectives to mitigate cyber security risk. Member States that already had cyber security strategies have begun to consider revising and modifying national strategies to incorporate the provisions of the NIS Directive into their strategic objectives. However, this is a small number of Member States, twelve of them - by the Year 2012 (when ENISA begun the process of supporting the EU Member States and EFTA countries to develop, implement, and evaluate their National Cyber Security Strategies), which developed cyber strategies (ENISA, 2018). Such support, Member States, nor potential Member States have not received in development of their national strategic documents regarding critical infrastructure protection and implementation of Directive 2008/114/EC. This is a good practice that should be transposed in that area as well. Nationally, with the aim to establish effective early warning mechanisms for threats, a various forms of Computer Emergency Response Team - CERT organizations were founded, as the points for the exchange and analysis of threat information. Information is exchanged not only in relation to cyber threats, but also for each defined sector of critical infrastructure, which additionally speaks about their interconnection.

However, the vulnerabilities in critical infrastructure are not only within EU Member States borders. A particular challenge for the Commission is encouraging candidate countries to adopt the same standards as Member States, for example in such areas as cyber-related legislation or the protection of critical infrastructure (European Court of Auditors, 2019:44). Additional efforts are done, but it also needs to be taken into consideration that lot of those countries has outdated systems and technology that can be ineffective to avoid possible attacks and achieve the expected level of resilience. As well, there is the lack of adequate measures and no coordination of critical infrastructure protection efforts (as many non-EU countries, some of them in SEE, don't have national CIP normative framework). Therefore, vital systems, objects and networks are exposed to various threats and in the need of comprehensive approach to develop CIP field. Having in mind the fact that you cannot protect something you don't analyze, evaluate and optimize it is at utmost importance for those countries to identify their critical infrastructure at national level (which is the process that was never done). The critical infrastructure field is evolving and getting refocused on the cyber critical infrastructure which demands even higher level of protection, so non-EU countries also need to consider the update of their national strategy on the protection of critical infrastructure, in line with the European and other inter and supra-national recommendations.

3. Legislative Frameworks – pre and after NIS directive

Quality concept of the national regulatory framework for information security is the basis for cyberspace regulation in the global environment (Klaić and Perešin, 2011). Accordingly, numerous countries have considered how to adapt their legislation in order to prepare for the emerging challenges. Different approaches have been developed until the consideration of creating horizontal legislation at EU level in order to protect the network and information systems across the Union based on a comprehensive and uniformed approach. In this article in several parts it is shown how and why the NIS directive was developed, its relevant provisions as well as the legislative that was existing before NIS directive - which is today the most relevant document for all Member States, as well as those countries that are in the pre-accession stages and want to steer their national efforts to achieve an adequate level of protection in their environment. Cyber threats, as well as other threats to critical infrastructure, are inevitable for every country in the world, regardless of its level of development. In order to give comparison what the Directive has changed in national legislative frameworks, firstly, the NIS Directive in general will be presented (its importance and obligations), and then the overview of national efforts (in analyzed countries) to achieve protection in the context of cyber (and infrastructure) security (their mechanisms and strategies).

The NIS Directive focuses on protection for Critical Information Infrastructures or national essential services, namely, through setting baseline security measures and implementing cyber incident notification. In addition, it stipulates the obligation to implement other technical and organizational measures for risk management and measures to prevent and minimize the effect of the incident on the security of network and information systems. Following those requirements, the

NIS Directive prescribes the EU Member States to adopt and implement a national strategy on the security of network and information systems (known as national NIS strategy). This national strategy must address a list of issues, including a risk assessment plan, a governance framework to achieve the objectives of the national strategy, the identification of measures relating to preparedness, response and recovery and others. But the main objective of the Directive is to provide a common level of security of network and information systems in all Member States (which was lacking before), having in mind that possible security incidents due to interconnectivity could have significant consequences on the whole community. NIS Directive also introduces an obligation for operators, to notify about incidents that may have a significant effect on the continuity of providing specific service. There are two types (groups) of actors to which directive implies - Operators of Essential Services and Digital Service Providers. The Operators of Essential Services are those who provide key services to society or the national economy in the seven sectors: Energy (electricity, oil, gas); Transport (air, rail, water, road); Banking, Financial Market Infrastructures, Health, Drinking Water Supply and Distribution, Digital Infrastructure (internet traffic exchange, domain name services, and national top level domain control). On the other side, the Digital Service Providers are legal persons that provide service in three sectors: Marketplaces, Cloud Computing Services and Online Search Engines. In this perspective there is the fundamental difference between operators of essential service and digital service providers – operators of essential services are affiliated with physical infrastructure, while digital service providers are more in the „wide space“ having cross-border (or even – no border) character.

The NIS Directive is part of a broad EU digital initiative which: promotes awareness on the need to develop the digital economy (in the relation to current process of creating an EU digital single market); enhances security awareness of cyberspace and reflects on a number of segments of modern society – including the development of public-private partnership and electronic services in public administration. Thereby, the NIS Directive creates appropriate framework for the prevention and protection of society against cyber threats by establishing a common approach of all Member States, as they individually ensure harmonized vertical sectoral approaches in terms of NIS Directive, while the new EU Personal Data Protection Regulation (GDPR) provides a similar horizontal approach through all segments of society as a whole (Government of the Republic of Croatia, 2018: 2).

The Republic of Croatia

Referring to the document of the Government of the Republic of Croatia from the introductory part of this chapter (which assesses the current situation (state -of-play) and presents the basic issues that need to be regulated by law), and which was made shortly before the adoption of the *Act on the Cyber Security of the Key Service Operators and Digital Services Providers* that implemented the NIS directive, it is evident that the importance of the European legislative framework has been understood with the full intention of implementation.

Drawing the parallel with the Croatian Cyber Security Strategy, which was adopted in 2015, it initially meets the necessary requirements set by the NIS Directive in relation to strategic national frameworks for the achievement of goals and requirements in cyberspace as a virtual dimension of society. The *Croatian National Cyber Security Strategy*, which was created in terms of recognizing the importance of national cybersecurity, says that “critical communications and information infrastructures are those communications and information systems that operate or are critical to the functioning of the critical infrastructure, regardless of which critical infrastructure sector is” (Government of Republic of Croatia, 2015). It is on the trail of NIS directive provisions, although it addresses the risks to network and information systems that support key services in designated sectors, where by the definition they cover a broad, general scope of all categories of possible incidents (failures, accidents and attacks), which can have a negative effect on the security of the network and information systems used in the providing of key services or digital services. What is significant and facilitates the implementation of regulations at national level is the existence of a detailed and structured Action Plan for the implementation of the National Cyber Security Strategy, but also the establishment of strategic and operational interdepartmental national bodies to manage the implementation of the strategy and address all relevant national cyber security issues. With the proposal of the *Act on the Cyber Security of the Key Service Operators and Digital Services Providers*, the strategy was expanded with additional requirements, aligned with the requirements arising from the transposition of the NIS Directive in the Republic of Croatia as an EU Member State.

In addition, the *National Cyber Security Strategy* and the *Action Plan for the Implementation of the National Cyber Security Strategy* have strongly highlighted critical infrastructure and its protection concept, most than all national strategies, assessments and plans to date. It was primarily perceived through critical communications and information infrastructures, which are defined as “communication and information systems whose malfunctioning would significantly disrupt the operation of one or more identified national critical infrastructures“. In the Strategy, a large amount of space is devoted to critical communication and information infrastructure coupled with cyber crisis management (Mikac, Cesarec and Larkin, 2018: 122). Also, the Strategy emphasizes the importance of the Critical Infrastructures Act and the necessity of achieving its provisions. It outlines five objectives that can be equally transferred to all sectors and are part of the context of the basic needs for implementing critical protection system procedures. These are: 1. To establish criteria for identifying critical communication and information infrastructure; 2. Identify binding security measures applied by the owners/managers of identified critical communications and information infrastructures; 3. Strengthen prevention and protection through risk management; 4. Strengthen public-private partnerships and technical coordination in the processing of computer security incidents (Government of the Republic of Croatia, 2015: 14-16). In accordance with the obligation of identification of critical infrastructure and all procedures that were also necessary but lacking in the implementation of the *Critical Infrastructure Act,* guidelines and prescribed criteria and thresholds were adopted for assessing the importance of the negative impact of an incident for critical communication and information infrastructure, that were also ultimately transferred to other sectors of critical infrastructure which are not designated by the *Act on the Cyber Security of the Key Service Operators and Digital Services Providers*. For the first time, cross-sectoral criteria for the needs of national CI identification have been adopted and have been successfully used. The above mentioned once again speaks of the interplay of these two normative documents in the Republic of Croatia.

Considering period before the NIS directive, according to Klaić and Perešin (2011: 690) who are bringing a hierarchy of information security regulations in the public sector, there are several levels: the first three levels constitute the implementation framework (implementation policies), with laws, regulations, internal acts and other documents prescribed by the Office of the National Security Council and information security advisers in the competent bodies, followed by internal implementing acts in government bodies and by the regulations of The Information Systems Security Bureau as the National CERT. The next three levels towards the top of pyramid is the legislative framework, that is, information security policies. These include the ordinances of the Office of the National Security Council on security checks, physical security (etc.), followed by the Law on the Security and Intelligence System of the Republic of Croatia, the Law on Security Checks, the Law on Data Confidentiality and the Decree of the Government of the Republic of Croatia. At the top of the pyramid, as a document setting strategic goals, was then the National Information Security Program (2005), which consists of 10 chapters defining information security, information security requirements from the aspect of international relations, the state of information security in the Republic of Croatia, segmentation of competences in relation to data and information structure in the Republic of Croatia, security policy, education and development of security culture), which is today replaced by the Cyber Security Strategy of the Republic of Croatia, as an umbrella document.

The main body responsible for cyber security in the Republic of Croatia is the “National Cyber Security Council” established in 2017 to achieve the Strategy's objectives and implement the Action Plan's measures as adequately as possible, and represents a platform for establishing and managing horizontal cyber security initiatives, both in the public sector and inter-sectoral. Also, the Council's purpose is to coordinate more effectively the prevention and response activities of cyber security threats in the context of a complementary approach to the prevention and resolving security incidents, and thus to the coordinate development of national capabilities in cyberspace. The work of the Coordination is coordinated by the competent body - the Ministry of the Interior, and it is directed by the “Office of the National Security Council”. The "National Cyber Security Council" is required to submit an annual report on the operational and technical coordination of cyber security in the Republic of Croatia.

As from the aspect of general critical infrastructure protection system in the Republic of Croatia, there was some challenges in achieving its functionality from perspective of inter-institutional cooperation and complexity of identification process, yet they are getting overcome by adapting national framework and by positioning CIP competent body at higher level of authority (from Administration State Body to the Ministry level). Also, the strategic direction in Republic of Croatia through implementation of guidelines set out by European Programme for Critical Infrastructure Protection policy and EU Cybersecurity policy has the prerequisites for achieving a successful critical infrastructure protection system.

Romania

Romania is facing various threats to critical infrastructure, mostly from cyberspace. This is due to an increasing interdependence between cyber infrastructure and infrastructure such as that belonging to banking, transport, energy and national defense sectors. The globality of cyberspace is likely to increase the risks affecting both citizens, businesses and the government (Government of Romania, 2013: 4).

From the legislative framework perspective (where the national strategy is the umbrella document), most relevant is the *Cybersecurity Strategy* adopted in 2013, which is setting out the principles for understanding, preventing and counteracting cybersecurity threats, vulnerabilities and risks. The main objectives of the Strategy are to adapt the regulatory and institutional framework to the threat dynamics of cyberspace and to establish and implement security profiles and minimum requirements for national cyber infrastructures, including the proper functioning of critical infrastructures. The

Strategy also highlights increased risks to citizens, businesses and the government, as cyber infrastructures face technical threats/failures, human threats and natural threats; puts in focus the resilience of cyber infrastructure; promote and develop co-operation between the public and private sectors at national and international level in the field of cyber security; sets preconditions to develop a security culture by raising awareness about vulnerabilities, risks and threats in cyberspace and the need to protect information systems; and also mentions the need to actively participate in initiatives by international organizations to which Romania belongs, as well as establishment of the international confidence-building measures concerning activities in cyberspace. According to researchers, in 2013, the Romania was one of minority of countries that defines all cyber-related notions in its national cyber security strategy, understanding it as: “normality resulting from applying a set proactive and reactive measures that ensure confidentiality, integrity, availability, authenticity and non-repudiation of electronic information, and the public and private resources and services in cyberspace“ (Luiijf et al., 2013: 6). In addition to national strategy, there is also a normative document developed for purpose of transposition of NIS Directive, adopted in January 2019, *Law no. 362/2018* concerning measures for a high common level of security of network and information systems. The National Defense Strategy of Romania (2015 - 2019) also emphasize relevance of cyber security of critical infrastructures, as the national security objectives include consolidating security and protection of critical infrastructures - including the cyber security sector. Strategy also recognizes the need to adapt critical infrastructures in relation to the occurrence of cyber attacks (The Presidential Administration of the Republic of Romania, 2015). It is relevant that necessity of CIP protection is recognized in wide range of national strategies, mostly because of multisectoral approach that needs to be applied in order to have adequate system for protection and resilience on (cyber) critical infrastructure. In that way it can be more easily achieved.

At the organizational level, the first step was taken in 2008 by the Romanian Intelligence Service, the Cyber-Intelligence National Authority (CYBERINT), which created the CYBERINT National Center as a platform for collaboration between institutions within the National Defense System and the interface with similar structures in NATO (Romanian Intelligence Service, Cyberintelligence, n.d.). The role of the Center is to prevent, analyze, identify and respond to incidents of cyber infrastructure that provide public utility functionality, develop and disseminate public policies to prevent cybercrime incidents and counteract incidents (Early Alert System and Real-Time Information on Cyber-Incidents) and provide advice to public authorities responsible for the identification and protection of critical infrastructure (Barbu, 2019: 52). From the strategic/operational level, the Romanian Intelligence Service, is the body responsible for the protection of state information and any network utilized by government entities in the possession of state secrets. The Cyber Security Strategy of Romania establishes two additional entities, which would act in conjunction to cover cybersecurity specific network and information security in Romania: “The National Cyber Security System” (SNSC) as a body composed of representatives from public institutions and tasked with the building and maintenance of a range of cybersecurity measures; and “The Operative Council for Cyber Security” which oversees the SNSC in its duties, as well as responding in the event of critical cybersecurity incidents. It is composed of representatives from Romanian government ministries and Romanian intelligence services (BSA, 2015.) In comparison with Republic of Croatia it is a similar approach in establishment of competent bodies for the implementation of national cyber security.

Regarding critical infrastructure protection system in general, Romania has transposed the spirit of Directive 2008/114/EC by the *Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures,* which regulates all national critical infrastructure sectors. It has organised processes, built a system of critical infrastructure protection, established functional forms of support to public institutions and owners or critical infrastructure operators in their tasks, and this works in practice (Lazari and Simoncini, 2014). In addition to the aforementioned policies and measures in the field of critical infrastructure protection, the Romanian Government has provided the basis for developing an adequate security environment with the aim of achieving the following strategic goals: 1) Ensuring unified procedures for the identification, designation and protection of critical infrastructure by leveling national and European critical infrastructure; 2) Operationalization of the national early warning system through the integration of all networks and existing information and organizational capacities; 3) accurate evaluation of the critical infrastructure vulnerability levels and identification of measures needed for preventive action and risk reduction; 4) development of cooperation at national, regional and international level in the field of critical infrastructure (Udeanu, 2015: 133). Additionally, in order to improve the transposition of the Directive 2008/114/EC and to ensure a better correspondence*, Law no. 636/2018* was adopted in November 2018 with focus on strengthen the role of the national critical infrastructure and European critical infrastructure owner/operator/administrator and give new attributions and responsibilities to relevant public authorities (Maravela, Popescu and Roman, 2018). It can be seen that Romania is adapting its framework accordingly to the recognized gaps which is applied on both perspectives – of cyber and physical critical infrastructure threats.

Montenegro

Montenegro as the EU candidate state (from June 2012) has its strategic orientation of critical infrastructure protection in the *Montenegro National Security Strategy* which was adopted in 2018, prioritizing development of efficient CIP system and strengthening of resilience. This initial step to organize national efforts in this field, is not the first existing legislation document that mentions CIP – it is also mentioned in various national laws, among which is the *Law on cyber security* adopted in 2016 (which defines security risk protection measures in information and communication systems, responsible legal entities in the management and use of information and communication systems and competent authorities for the implementation of protection measures, coordination and monitoring of the application of the main security regulations). There are also some recent strategical documents related to CIIP such as *Strategy on Cyber Security (2018-2021)*with the aim to strengthen capacities for the IT critical infrastructure protection, and generally security of infrastructures. It identifies eight IT critical infrastructure sectors and brings critical information and technology infrastructure definition, as the „information systems whose disruption or destruction could jeopardize life, health, safety of citizens and state functioning or from whose functioning depends public activities“ (Government of the Republic of Montenegro, 2017:14). Additionally, it includes provisions on: Modern risks, threats and challenges; Retrospect (from the first Cyber Security Strategy until today); National organizational structure; National cyber defense, including cyber capabilities, critical IT infrastructure, inter-institutional cooperation, data protection, education, public-private partnership, regional and international cooperation; and Monitoring. As mentioned, the first *Montenegro Cyber Security Strategy (2013-2017)* had its main objectives of: 1. Defining institutional and organizational structure in the field of cyber security in the country; 2. Protection of critical information structures; 3. Strengthening capacities of state law enforcement authorities; 4. Incident response; 5. Define and strengthen the role of Ministry of Defense and Military in cyberspace; 6. Public-private partnership; 7. Raising public awareness and protection on the Internet, which has put in focus majority of challenges and fields of regulation that are also taken in consideration in whole EU level (Government of the Republic of Montenegro, 2013).

By available researches, the establishment of the “National council for cybersecurity/information security“ as the competent body was planned by first Cyber Security Strategy in 2013, yet, it was not achieved. Once operational, the Council is supposed to be the key institution related to cybersecurity issues. The Council will also be in charge of creating procedures for the regular exchange of information between state authorities and key institutions from the private sector, i.e. internet providers, agents for .me domain, banking sector, electric power companies and companies that host e-services in Montenegro (Minović, et.al. 2016:20). In some terms form perspective of cyber security - the direction and coordination of the work of the bodies constituting the intelligence and security sector is carried out by the National Security Council, and the operational coordination and harmonization of the activities of the bodies that constitute the intelligence and security sector is performed by the Bureau for Operational Coordination (Government of the Republic of Montenegro, 2018:23). There is an operational importance of establishment of competent bodies so the implementation of processes can be monitored, which can be perceived as one of the “weak points” of cyber security in Montenegro.

Considering the general preconditions of national CIP framework – adequate legislation, the most relevant document for CIP in Montenegro was adopted in December 2019, *Law on determining and protecting critical infrastructure*, bringing definition of critical infrastructure, CI sectors, criteria for identification, obligations of stakeholders and all other issues relevant to critical infrastructure system regulation. It also regulates the area of European critical infrastructure, since the provisions of this chapter will apply upon the accession of Montenegro to the European Union. Since the law is newly adopted, we can conclude that the system of critical infrastructure is still under the development in Montenegro, and the applicability of presented framework could not be analyzed – procedures for CIP yet needs to be evolved.

The Republic of North Macedonia

North Macedonia has a candidate status since 2005 and through the efforts in establishment of national security framework its tendency to implement all EU standards in security field is very visible. The focus of protection of critical infrastructure from national perspective is in energy sector, information technologies, water systems and air traffic (Mitrevska, Mileski and Mikac, 2019:143) – each of them regulated by their Laws which provide the wide range of measures. In general concept of CIP, North Macedonia doesn't have formal framework, but it has the basis in strategic and normative documents in the field of defense and security, such as: *National Cyber Security Strategy of the Republic of North Macedonia, (2018-2022)*, *Law on Internal Affairs, Crisis Management Law, Protection and Rescue Law and Law on Private Security* (Mitrevska, Mileski and Mikac, 2019:146).

National Cyber Security Strategy can be perceived as the initial process and willingness to establish CIP system. The Strategy mentions critical infrastructure as prone to cyber incidents and emphasize these threats as one of the most serious in terms of national security. It also considers critical communications and information infrastructure in terms of cyber crisis management - the need to strengthen national capacities for cyber security prevention and protection, and implement activities to raise national cyber security awareness. The Strategy defines cyber-physical threats to critical infrastructure, such as: increased number of cyber-attacks, including industrial cyber espionage, cyber vandalism and vulnerability identification in the energy sector, transport systems and other parts of the Critical Information Infrastructure. In terms of competent authorities to monitor implementation of cyber security and through that the protection of cyber-physical threats to critical infrastructure, establishment of such body is was on of the priority activities of *National Cyber Security Strategy.* "The National ICT Council" was established in February 2018 to prepare and monitor the implementation of the National ICT Strategy, and at the end of 2018, the Government of Republic of North Macedonia made a strategic decision to establish the "National ICT and Cyber Security Council", and extending responsibilities, members and authority of the existing „National ICT council". "The National ICT and Cyber Security Council" consists of relevant ministers, thereby ensuring compliance of strategic-level decisions across state institutions (European Commission, 2019:15).

From perspective of CI in other sectors, there are not such strategically oriented documents, yet some legislation, such as previously mentioned the *Law on Internal Affairs* (regulates the obligation of the police to protect important objects that are specific, i.e. part of critical infrastructure); and the *Law on Private Security* (which prescribes which legal entities are obliged to private security – in their activities which can jeopardize people, environment, objects and facilities of particular cultural and historical importance and in other cases when it is in the interest of the security) – can be perceived as nationally established forms of critical infrastructure that are not defined in the means of Directive 2008/114/EC (which is adapted and/or transmitted by Member States), but are nevertheless identified and recognized as objects of national importance. Despite of that, it is visible that there is no comprehensive regulatory framework for the management of such facilities. There is no legislative document that would solely (and specifically) deal with critical infrastructure protection system. Therefore, a formal framework needs to be adopted in order to build a critical infrastructure protection system in a whole.

4. Recommendations for future (cooperation in critical infrastructure protection and dealing with gaps in achieving cyber-security)

Critical infrastructure protection, both physical and information-communication is a complex and challenging job. That is one of the many reasons why the public sector (governments, legislators, etc.) cannot effectively work on raising the level of resilience and protection without cooperation with representatives of the private sector (who are majority owners/operators of critical infrastructure in most countries), NGOs, the scientific community and experts in specific areas of information and national security. Cooperation of the public and private sector, must be especially emphasized, where due to the competences that the private sector has (in critical infrastructure management) it must face challenges in achieving critical infrastructure protection (e.g. implementation of security measures requiring the investment of additional resources). In the foregoing, the public sector must support them, whether through deductions or other benefits that are achieved through public-private partnerships as one of the fundamental pillars of cyber security policy.

Consequently, it is important to highlight cyber security public policies as one of the main tools for achieving cyber security. The foundation of national information security is in the development of protection policies, strategies and action plans in case of incidents which are compromising data, and/or functionality of infrastructures. Achieving cybersecurity is complex task that requires multi-level involvement of mechanisms that should also be included at the governmental level in public policy. Not only on national level, it is equally important for stronger resilience to adopt coherent public policies for EU level on coordinated cross-sectoral action and trans-sectoral cooperation mechanisms which can ensure security in the whole community. Also it is important to have forms of establishment of cooperation with EU (as well as non-EU members), such as bilateral and multilateral agreements, memorandums of understanding, commitments between the competent authority and international strategic partners in the public, private and academic sectors. The example of such cooperation is formal agreement on stance, for example "Joint Statement, Visegrad (V4)-Austria, Croatia, Slovenia" where the cyber security is identified as one of the issues to take action (Ministry of Foreign Affairs and Trade of Hungary, 2017) through the cooperation of SEE countries and other Member States.

The next set of recommendations is related to the development of joint regional cybersecurity capabilities which can foster sharing of information about threats to cybersecurity (including early warning systems); development of tools and techniques; exchange of experts and best practices – to have better and faster reaction in case of a cybersecurity incident which could affect the region. On that note, joint workshops, trainings and exercises not only in SEE region but also on European level can be very useful to test national mechanisms and see how they function before the real event of a cyber incident. For that purpose, large scale and sophisticated attacks can be simulated as well as failure modes for recognized vulnerabilities. As an example of such exercises, we can take exercises conducted by the European Network and Information Security Agency (ENISA) – in 2018, "Cyber SOPEx" was held with the aim of improving cooperation between national Computer Security Incident Response Teams and a focus on raising awareness of information sharing. understanding the roles and responsibilities within the team and use of tools needed to successfully handle incidents; and

“Cyber Europe 2018“ organized by ENISA in collaboration with cyber-security bodies and agencies across Europe, with 900 European cyber-security experts from 30 countries facing the scenario of intense cyber-security incident at the airport as critical infrastructure.

The Education is the next segment of recommendation, and previously mentioned agency ENISA has activities to facilitate education and general awareness which will promote NIS skills and support the Commission in enhancing the competence of professionals in this area. It also provides Guidelines such as: “Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity“ (2019), overviews and reports (like “Status of privacy and NIS course curricula in EU Member States“ (2015) which can be used as transfer of best practice), etc.

As an additional opportunity for Member States but also non-EU countries are EU funds and project implementation (such as the Collaborative research and innovation projects) which can be used for enhancing security and resilience for national purposes, as well as the region and wider space of EU community. As part of the implementation of the NIS Directive, it is planned to use EU funds, where the most referenced is "Connecting European Facilities" – CEF. Through the CEF Cybersecurity calls EU seeks to support the EU Member States in putting the NIS Directive's legal provisions into practice. Between 2016 and 2017 the European Commission has awarded €18 million funding - mainly to CSIRTs (Computer Security Incident Response Teams provide support services to handle cybersecurity threats and incidents for national stakeholders (in public sector, operators of essential services, critical infrastructure entities and digital service providers) to 19 EU Member States. Since 2018, following the transposition of the NIS Directive into national legislations, the possibility of applying and using the CEF Fund to legal entities - sector operators, through the competent sector bodies, has been given, which is additionally significant for further capacity development. Also, there is a call for proposal under the Horizon 2020 Programme (which is of particular interest to SEE countries, as the analysis in this research has shown, are mostly still focused on strengthening the physical protection system of critical infrastructures - with a tendency to consider cyber security), called “Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe“ where SEE countries already participate in projects: SATIE - *Security of Air Transport Infrastructure of Europe* (Croatia), InfraStress - *Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats* (Slovenia) which is especially interesting because of open testbed stress-testing system as a concrete activity under project implementation.

As it can be seen in this chapter, there are wide range of possibilities set out to all countries that are willing to invest time and efforts to build concrete cooperation in CIP and CIIP all in the aim to overcome the gaps between more developed and slightly less developed countries in terms of security culture – by exchange of knowledge and best practices fostered by listed recommendations.

5. Conclusion

National critical infrastructure protection cannot be achieved without adequate protection of cyberspace through which all data related to the operation of critical infrastructure flows - either through their exchange or storage. That is why this dependence on information and communication technology requires that cyber-security measures are prescribed and regulated by national legislation – to enable systems, networks and object of critical infrastructure to be able to detect, prevent and effectively respond to security threats in a timely manner.

An essential element is also cross-sectoral compliance, which requires well-coordinated management and security mechanisms and separation of roles between data owners, infrastructure owners and users so that obligations can be prescribed and systematic approach achieved. A comprehensive perspective is important, because segmented solutions could affect the balance of the processes and the overlapping of authorities in terms of cyberspace and the perception of physical protection, which is a possible challenge in SEE countries that generally perceive the two areas separately. In that perspective, we can refer to our national (Croatian) example where the challenge is to effectively coordinate the processes related to the implementation of the *Critical Infrastructure Act* and the *Cyber Security of the Key Service Operators and Digital Services Providers Act*, since there may be overlapping of responsibilities, unnecessary waste of resources and delays in implementation due to the lack of clarity in the implementation of security measures (what level of protection for which area), but also the reluctance of stakeholders to whom are prescribed obligations in both laws that are equally comprehensive and because of that one will be completed and the other not - although they are very similar. It is interesting to see that non-EU countries have "skipped step" and regulated the cybersecurity area that mentions information and communication critical infrastructure rather than they regulated the critical infrastructure area as prescribed by Directive 2008/114/EC. One of the perspectives on this occurrence is the fact that these countries already protect and have identified infrastructures of national importance (without being specifically named “critical infrastructure“) - as we can see in the analyzed countries (Montenegro and North Macedonia), but they don't have pre-existing mechanisms of protection in cyberspace, which is a contemporary challenge that has major negative effects if a security incident occurs.

In the part of considering critical infrastructure protection from cyber threats, it is determined that it is a complicated matter and therefore it must be included in national preparedness planning, as well as in recovery planning of individual infrastructures of national importance. Despite identifying potential threats and taking security measures, the level of resilience and security may not be fully satisfactory, as the threats are increasingly modified (such as hybrid threats) and become an additional challenge to cope, often exceeding national capacities and seeking international cooperation. The European Union, as a supranational community analyzed in this paper (although the NATO Alliance, for example, develops its own mechanisms), takes cyber security issues extremely seriously, placing it as one of the top priorities of modern security. According to European Commission guidance, Member States have significantly stepped up the implementation of activities to take action and organize organizational elements to deal with cyber threats, reinforcing existing mechanisms and legislative frameworks or creating new ones (if they did not exist before). Countries that are not EU Member States, followed their steps, recognizing the need to protect critical infrastructure and all the data it has, especially since cyberspace has no boundaries and cannot be monitored comprehensively so it seeks segmented protective actions. Therefore, it is nationally important to build cyber defense capabilities through education and training, various exercises and workshops, the development of information sharing mechanisms and the synergy of various professional organizations at national and international levels.

The analysis in this paper shows that there are efforts in the region to achieve a higher level of security in national systems that are most important for the functionality of the community, i.e. critical infrastructure, however, are in line with the capacities and capabilities of states – if there is no adequate protection against environmental impacts that affect the physical components of the infrastructure and sufficient awareness (usually at the strategic level), it is difficult to achieve influence on the creation of collective risk awareness in virtual space. Implementation challenges often stem from lack of knowledge how to implement processes which are prescribed by legislation, so sharing knowledge and experience is a good opportunity to bridge the gap in cybersecurity development for the benefit of the entire community, region and the global environment as a whole.

6. References

BSA The Software Alliance (2015) EU Cybersecurity Dashboard Country Report – Romania, URL: http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_romania.pdf , accessed 13 February 2020

Croatian Parliament (2018) Act on the Cyber Security of Key Service Operators and Digital Services Providers. Official Gazette (64/2018), https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html (Croat.), accessed: 5 February 2020

ENISA (2015) Status of privacy and NIS course curricula in EU Member States, https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states , accessed: 10 February 2020

ENISA (2018) ENISA launches the Cybersecurity Strategies Evaluation Tool, URL: https://www.enisa.europa.eu/news/enisa-news/enisa-launches-the-cybersecurity-strategies-evaluation-tool, accessed: 10 February 2020

ENISA (2019) Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity , accessed: 10 February 2020

European Commision (2013) Joint Communication to the European Parliament, the Council the European Economic and Social Committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf , accessed: 17 January 2020

European Commision (2019) Digital Government Factsheet 2019- Republic of North Macedonia,https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_North_Macedonia_2019.pdf , acessed 15 January 2020

European Commmission (2017) Joint Communication To The European Parliament And The Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 , accessed: 11 January 2020

European Court of Auditors (2019) Challenges to effective EU cybersecurity policy, URL: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBER S ECURITY_EN.pdf , accessed: 13 January 2020

European Parliament and the Council of the European Union (2016) Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, EUR-Lex, Official Journal, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&amp;from=EN , accessed: 11 January 2020

Goverment of Romania (2013) Cyber Security Strategy, https://cert.ro/vezi/document/NCSS-Ro , accessed: 13 January 2020

Goverment of Romania (2019) Law no. 362/2018 on ensuring a high common level of security of network and information systems https://www.wolftheiss.com/fileadmin/content/6_news/clientAlerts/2019/2019_Q1/19_01_23_CA_Romania_New_Law_362-2018_Bucharest.pdf , accessed: 13 January 2020

Goverment of the Republic of Croatia (2018) Proposal of Act on the Cyber Security of the Key Service Operators and Digital Services Providers https://vlada.gov.hr/UserDocsImages//2016/Sjednice/2018/03%20o%C5%BEujak/86%20%0sjednica%20VRH//86%20-%204.pdf , (Croat.), accessed: 5 February 2020

Government of the Republic of Croatia (2015) Croatian National Cyber Security Strategy, Official Gazette (108/2015) https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html, (Croat.), accessed: 10 February 2020

Government of the Republic of Montenegro (2013) Cyber Security Strategy 2013-2017 http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=165416&rType=2&file = Cyber%20Security%20Strategy%20for%20Montenegro.pdf , accessed: 10 January 2020

Government of the Republic of Montenegro (2017) Cyber Security Strategy 2018-2021, http://www.mju.gov.me/ResourceManager/FileDownload.aspx?rid=305198&rType=2&file= Cyber%20Security%20Strategy%20of%20Montenegro%202018-2021%20eng.pdf , accessed: 10 January 2020

Government of the Republic of Montenegro (2018) National Security Strategy, http://www.mod.gov.me/ResourceManager/FileDownload.aspx?rid=381268&rType=2&file= Strategy%20of%20National%20Security%20of%20Montenegro%20With%20the%20Action %20Plan.pdf , accessed: 10 January 2020

Government of the Republic of Montenegro (2019) Law on determining and protecting critical infrastructure, Official Gazette (72/2019) https://me.propisi.net/zakon-o-odredjivanju-i-zastiti-kriticne-infrastrukture/, accessed 15 February 2020

Government of the Republic of North Macedonia (2005) Law on Crisis Management, Official Gazette (29/2005) https://www.refworld.org/docid/5d31a0c37.html , accessed: 15 January 2020

Government of the Republic of North Macedonia (2012) Law on Protection and Rescue, Official Gazette (93/2012) http://www.slvesnik.com.mk/Issues/1F2D347B699C764F9E65C717889E74B2.pdf accessed: 15 January 2020

Government of the Republic of North Macedonia (2018) National Cyber Security Strategy of the Republic of North Macedonia (2018-2022) http://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf , accessed: 5 January 2020

Marvela, Popescu and Roman (2018) New Provisions Concerning Critical Infrastructure in Romania, URL: https://www.legal500.com/developments/thought-leadership/new-provisions-concerning-critical-infrastructure-in-romania/ , accessed: 7 February 2020

Mikac, R., Cesarec, I., Larkin, R. (2018) Critical Infrastructure - A Platform for Successful Development of Nations Security, Zagreb: Jesenski i Turk, (Croat.)

Ministry of Foreign Affairs and Trade of Hungary (2017) Joint Statement of the Ministers of Foreign Affairs of the Visegrad Group, Austria, Croatia and Slovenia, URL: http://www.visegradgroup.eu/calendar/selected-events-in-2017-170203/joint-statement-of-the-170710 , acessed: 5 February 2020

Minović, et.al. (2016) Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, Geneva: Diplo Foundation - Research report under the project "Cybersecurity Capacity Building and Research Programme for South-

Eastern Europe" implemented with the support of the Federal Department of Foreign Affairs of Switzerland, URL: https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.p df

Mitrevska, M., Mileski, T., Mikac, R. (2019) Critical infrastructure – concept and security challenges, Skoplje: Friedrich Ebert Foundation

Perešin, A., Klaić, A. (2010) The Connection of Critical National Infrastructure and Data Protection Concepts, Velika Gorica: Book of Papers, 3rd International Conference "Crisis Management Days", University of Applied Sciences Velika Gorica (pp. 13-29), (Croat.)

Perešin, A., Klaić, A. (2012) The role of cyber security in critical infrastructure protection, Velika Gorica: Book of Papers, 5th International Conference "Crisis Management Days" University of Applied Sciences Velika Gorica (pp. 335-355), (Croat.)

The Coundil of the European Union (2008) Council Directive 2008/114/EC of 8 December2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, 2008/114/EC, EUR-Lex, Official Journal, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF accessed: 13 January 2020

The Presidential Administration of the Republic of Romania (2015) National Defense Strategy 2015-2019: A StrongRomania within Europe and the World, URL: https://www.presidency.ro/files/userfiles/National_Defense_Strategy_2015_-_2019.pdf, acesssed: 14 March 2020

Tofan, D., et.al. (2016) The cost of incidents affecting CIIs: ENISA https://www.enisa.europa.eu/publications/the-cost-of-incidentsaffecting-ciis, accessed: 17 January 2020

Udeanu, G. 2015. Opinions regarding the new challenges to the critical infrastructures. International Conference Knowledge-based Organization 21(1):127–134. https://www.degruyter.com/view/j/kbo.2015.21.issue-1/kbo-2015-0021/kbo-2015-0021.xml, acessed: 14 March 2020.

World Economic Forum (2017) The Global Risk Report 2017, 12th Edition, URL:http://www3.weforum.org/docs/GRR17_Report_web.pdf , accessed: 15 January 2020

[1] The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.