CRITICAL INFRASTRUCTURE

CONCEPT AND SECURITY CHALLENGES

Marina Mitrevska
Toni Mileski
Robert Mikac

FRIEDRICH EBERT STIFTUNG

MARINA MITREVSKA
TONI MILESKI
ROBERT MIKAC

CRITICAL INFRASTRUCTURE: CONCEPT AND SECURITY CHALLENGES

Skopje, 2019

Content

Preface

Around the end of this year, which marks the 70th anniversary of NATO's foundation, the Alliance member states are expected to complete their national ratifications of the NATO Accession Protocol with the Republic of North Macedonia, making it officially the latest and 30th member state of the Alliance.

Aside from producing a variety of security, as well as economic and social benefits for each member state, being part of NATO also implies a lot of hard work, commitments and obligations for each segment of Macedonian society – the citizens individually, the institutions, organizations, and everyone else. This particularly comes to the fore when it comes to the issue of improving the rule of law and the independence of the judiciary, as well as boosting the development of the education and healthcare system in the country

It is precisely for these reasons that the Friedrich-Ebert-Stiftung decided to provide its input to this process by lending its support to certain endeavours that could prove useful to both the country as a whole and the individual sets of policies it will be pursuing over the next stages of its integration into NATO. The topic of critical infrastructure protection was brought forward in this context by the group of academic authors who co-wrote this publication and, after an inclusive process involving public debates and experts presenting their views on this matter, the final version of the material on critical infrastructure protection eventually saw the light of day.

Using Croatia as an individual example, it was vital to do case studies on newer member states of the Alliance, thus drawing on the experiences and learning of their own process of integration into NATO and how they have been functioning as full-fledged member states of the Alliance. Sharing experiences and good practices in this manner will be vital at this point when the country is going through the final stage of acceding to NATO, as well as in the months and years to come after the official accession when policies will start taking shape and be put into operation.

Having been put together to provide a presentation and elaborate upon all aspects of critical infrastructure protection, as well as to encourage activities to create a national strategy and ultimately adopt a law on critical infrastructure protection in the Republic of North Macedonia, we sincerely hope that this publication will draw the interest of the expert community in the country with regard to this matter and will prove to be of particular use to the relevant institutions when dealing with it going forward.

Nita Starova
Friedrich-Ebert-Stiftung Skopje Office

Introduction

The idea of writing a book like the one in front of you, entitled ***"Critical Infrastructure: Concept and Security Challenges"*** is a bold scholarly and erudite step. We have directed our long-term scientific and research career to several premises. The first basic premise of this book begins with the concept of critical infrastructure as a general set of values and goods that are essential to the economy, the state and the society. Disruption or destruction of such values and goods could have long-term detrimental effects on the core values of the society. Consequently, when creating a modern concept of critical infrastructure protection one recognizes the need to build a coordinated approach.

The second premise that characterizes this book is aimed at showing that the security problems faced by the states today have reached a level of seriousness and urgency. In such situations, it is understandable that quick fixes and ad hoc solutions are not enough and therefore it is necessary to consider actions that will help, or require an effective way of changing the approach to critical infrastructure protection.

The third basic premise of this book is the domain of critical infrastructure protection at national level, that is, individually and for this purpose we have singled out the examples of the United States and Croatia and the polices and processes that the EU and NATO have initiated and are striving to coordinate. These experiences are deemed valuable for future directions in the creation of the critical infrastructure protection system in the Republic of North Macedonia.

In the interest of a comprehensive analysis, we have also included two eminent foreign critical infrastructure experts, namely, Richard Larkin and Matthew Vatter. Their participation in this project, through their analysis of critical infrastructure protection in the United States, adds particular importance to the book in seeking a meaningful solution in the creation of a critical infrastructure protection system in the Republic of North Macedonia.

The content of ***"Critical Infrastructure: Concept and Security Challenges"*** is systematized in six chapters.

Within the **first chapter** entitled ***"Critical Infrastructure: Notion and Concept"***, the emphasis is put on the notional determination of infrastructure as critical. In this context are also elaborated the threats on critical infrastructure and the need for critical infrastructure protection. Furthermore, this part also includes a section referring to the analysis of the Critical Infrastructure Indicative List.

In the **second chapter** entitled ***"Critical Infrastructure Protection in the European Union"***, the focus of the research is dedicated to the development of critical infrastructure protection from the perspective of the European Union, the work of the Union's institutions and the orientation of this domain for cooperation with the private sector. This part also covers the section concerning Directive 2008/114/EC on the identification and determination of European critical infrastructures and the assessment of the need to improve their protection.

In the **third chapter** entitled ***"Critical Infrastructure Protection in NATO"***, the focus of interest is the Alliance's place and role in critical infrastructure protection and through critical analysis of a segment of NATO's involvement and role in critical infrastructure protection an attempt is made to tackle several important issues. One of them is whether NATO is conducting excessive securitization and militarization of the energy sector, which is dominantly perceived as an exceptional economic issue and whether there is an appropriate role and opportunity for engaging NATO in critical infrastructure protection within the framework of strategic concepts, especially after the end of the Cold War.

Within the **fourth chapter** entitled ***"Critical Infrastructure Protection in the United States"***, the emphasis is put on analyzing one of the leading countries in the development of critical infrastructure protection. In this context, the concept and system of critical infrastructure protection with the three basic segments the functional, political and technical mechanisms for critical infrastructure protection are very carefully elaborated.

In the **fifth chapter** entitled ***"Critical Infrastructure Protection in Croatia",*** the achievements in the development of critical infrastructure in Croatia made so far have been analyzed. In this context, Croatia's approach has been elaborated upon adoption of the Law on Critical Infrastructure Protection and bylaws, as well as the organization of the critical infrastructure protection system.

The **sixth chapter** entitled ***"Republic of North Macedonia and Critical Infrastructure Protection",*** provides an overview of the current situation in the Republic of North Macedonia related to building an efficient system for critical infrastructure protection. This section identifies priority sectors of critical infrastructure such as energy, information technologies, water systems and air transport. In each of the sectors mentioned, as a result of the reform efforts of the state, there are certain laws and bylaws that can enable effective regulation of critical infrastructure protection. Based on such situations, appropriate measures and recommendations are being offered that would be most useful in the organization of critical infrastructure protection. As an example, the ways and opportunities for creating an effective strategy for protection of critical energy infrastructure are offered. The strategy, after identifying the existing risks, should provide the right direction to overcome the situation of lack of positive legislation on critical energy infrastructure. However, the authors emphasize that partial solutions have been identified in different sectors of critical infrastructure, which are not faulty but are likely to contribute to "stifling" the entire process of designing and efficient functioning of the optimal system for critical infrastructure protection. As a result of such situations, at the end of the chapter, broader recommendations have been given that should outline practical steps towards building an effective system for critical infrastructure protection.

We express our gratitude to the reviewers Professor Jonas Johansson, Director for Critical Infrastructure Protection Research, Lund University, Sweden and Professor Roberto Setola, Univertsita Capmus Bio-Medico di Roma, Italy, for presenting us with the honour of accepting to peer review this manuscript, and their knowledgeable, academic and sincere support for the publication of this book.

Our deepest appreciation go to the "Friedrich-Ebert-Skopje" Foundation for helping us with this project and for the publication of this book in Macedonian and English.

The authors remain thankful for all well-intentioned suggestions, which will be considered in the next edition.

The authors
Skopje, August 2019

CHAPTER 5

CRITICAL INFRASTRUCTURE PROTECTION IN CROATIA

CHAPTER 5

Critical Infrastructure Protection in Croatia[12]

Robert Mikac, PhD
Faculty of political science of the University of Zagreb

The chapter provides an insight into the current development of this area in the Republic of Croatia. Until its entry into the European Union in 2013, the Republic of Croatia devoted a certain amount of attention in strategic and enforcement documents to critical infrastructure but did not set up a rounded normative framework of legal and subordinate legislation to begin the process of developing critical infrastructure protection system. Immediately prior to the entry into full EU membership, Croatia adopted the *Critical Infrastructure Act* and set the required initial normative framework for starting the purposeful development of this area (Government of the Republic of Croatia, 2013a). The aforementioned systemic Act has become the foundation for further development of this area and the initial step towards building a critical infrastructure protection system.

Since then, the establishment of a strategic and normative framework for critical infrastructure protection has taken place in three phases, which is important to point out because through the realized documents, processes and events in each phase, the desired system of critical infrastructure protection in the Republic of Croatia is gradually being build and developed. It is also important to emphasize that the Croatia currently does not have a critical infrastructure protection system which is fully set up – there are outlines – and significant efforts for its implementation. Normative background has been made, key actors are known, processes are established, but the underlying challenge is the insufficient coordination.

In this overview and analysis – key activities done by the Republic of Croatia will be presented, as well as a review of these processes and what could be done, all in order to extract identified lessons that may be useful from the planning positions of the strategic, normative and operational framework for the critical infrastructure protection in the Republic of Northern Macedonia, for which this analysis was carried out. The time period of the analysis is from 2008 to the end of 2018, where all the events are chronologically sorted and analyzed to follow the development phases, their replenishment and the finding of new solutions.

The structure of the chapter is divided into four sections: 1. The period till the entry into the European Union in 2013; 2. Establishment of the regulatory and strategic framework for critical infrastructure protection, covering the period

12 The initial research of this area related to the complete presentation and analysis of activities in the Republic of Croatia was written for the needs of book Mikac, R.; Cesarec, I. and Larkin, R. (2018), *Critical Infrastructure: The Platform for Successful Nation Security*, Zagreb: Jesenski and Turk.
For the purposes of this research, the text has been revised and supplemented.

from 2013 to the end of 2018; 3. Structural challenges in establishment of critical infrastructure protection system; 4. Conclusion. They are ordered from more general to more complex to show the breadth of the areas and challenges in establishing a critical infrastructure protection system.

5.1. The period until the entry into the European Union

During the last ten to fifteen years, the Republic of Croatia is working on the normative and strategic arrangement of the area of strengthening the resilience and protection of critical infrastructures. Until entering the European Union, the Republic of Croatia has identified the importance of identifying and protecting critical infrastructures in various strategic documents as well as in certain laws. These will be chronologically analyzed and their most significant parts will be highlighted.

In the *National Strategy for the Prevention and Countering of Terrorism* from 2008, critical infrastructures concept was perceived from the aspect of protection against terrorist threats. As stated in the strategy: "In principle, a terrorist threat may vary between individual attacks on highly symbolic values, attacks aimed at causing as many victims as possible, spreading more intense fear and greater scale of destruction, and attacking critical national infrastructure. Critical national infrastructure consists of assets, services and systems (transport, energy, communications, industrial, financial and administrative) that support economic, political and social life in the Republic of Croatia, whose importance is such that its total or partial loss or threat can cause large human losses, have a serious impact on national security and the economy, and have other serious consequences for the community as a whole or any part of the community" (Government of the Republic of Croatia, 2008: item 8). The Strategy in the terrorism protection segment points out that the Republic of Croatia needs to build national capabilities to protect critical infrastructure.

The 2010 *Protection and Rescue Plan* for the Republic of Croatia, as the most important document for the planning of protection and rescue operational forces operations, and the organization of the civil protection system in response to major accidents and disasters – is mentioning critical infrastructure in the context of overview of the obligations that the participants involved in the implementation of protection and rescue measures have. Therefore, the Plan does not provide a definition of critical infrastructure, although the concept appears within the scope of the obligations (protection and rescue measures) of the participants of civil protection system through the determinants of protecting vulnerable (endangered) critical infrastructure facilities (in case of flooding) and restoring critical infrastructures facility functions (in case of earthquakes). With regard to the implementation of the Plan, one of the important aspects of the application is the "planning of procedures, bearers, sources of financing and coordination of reconstruction of damaged and destroyed basic resources and critical infrastructure facilities, as well as for defining the concept of the whole renewal of the community affected by the disaster and large scale accident" (Government of the Republic of Croatia, 2010: item 6).

The 2010 *Private Protection Act* defines critical infrastructure as "activities, networks, services and goods of material and information technologies whose failure or destruction would have a significant impact on the health and safety of citizens or the effective functioning of state power" (Croatian Parliament, 2010). The state under the normative framework stipulates that critical infrastructure facilities should be protected, but the owner/manager decides in what way. Given the fact that private security companies have significant asset protection capabilities (not only with human resources but also technical solutions) they are engaged to ensure a high level of system security, primarily in the prevention segment.

Risk Assessment for Republic of Croatia from Natural and Technical-Technological Disasters and Major Accidents (2013), puts critical infrastructure in wider range of protection from natural and anthropogenic threat sources. Within this document, the concept of critical infrastructure protection is mentioned ... "and what is the common name for the networks and systems crucial to the functioning and life of the community, whose damage or destruction can provoke temporary or long-term disruption and crisis, is of particular interest and importance to The Republic of Croatia as a whole, but also partially for the units of local and regional self-government" (Government of the Republic of Croatia, 2013b: 72). The Risk Assessment states that "critical infrastructure in the Republic of Croatia is not defined nor the need to protect it and ensure the continuous operation in the Republic of Croatia is assessed in all, especially in emergency situations, therefore a proposal of the Critical Infrastructure Act has been drafted, taking into account the acquis of the European Union contained in *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection* (Official Journal of the European Union L345/75, 23.12.2008) and harmonization of national legislation with that European Union regulation" (Government of the Republic of Croatia, 2013b: 73). The Risk Assessment draws attention to need of raising the level of critical infrastructure security that will enable the future normative framework and what that framework should prescribe and provide.

The National Strategy and Action plan for the Non-Proliferation of Weapons of Mass Destruction (2013) is mentioning the critical infrastructure protection and the population from the crisis caused by the mass destruction as a specific objective (Government of the Republic of Croatia, 2013c). In addition to that provision, subject matter is not further elaborated.

Although there is a clear interest in normative framing of concepts related to critical infrastructure, none of the documents provided a complete solution for risk management of critical infrastructure operations and protection framework, primarily because it was not the main objective of the mentioned documents (Mikac and Cesarec, 2019). During the period until entry into the European Union, the interest of legislators and various experts in this area was noticeable. Everyone agreed that there is a need to establish the specific area dedicated to critical infrastructure development, since critical infrastructures were at that time part of the protection and rescue, protection against terrorism and the protection of weapons of mass destruction area, as an instrument in the implementation (supplement) of the relevant policies and did not have the wholeness in the necessary consideration and articulation.

5.2. Establishment of a regulatory and strategic framework for critical infrastructure protection

Processes related to building of critical infrastructure protection system took place in three time periods/cycles. The first, marked by the obligation to nationally regulate the protection of European and then critical national infrastructures, where the central event is related to the adoption of the Critical Infrastructure Act during 2013. The second time period from 2014 to 2015 is marked by the adoption of the updated *National Strategy for Prevention and Countering Terrorism* and the *National Cyber Security Strategy*, where both strategies, especially the second one, emphasized the importance of continuing the activities in the area of critical infrastructure protection towards the establishment of a comprehensive protection system. The third, which took place over the period from 2016 to 2018, when the following documents were adopted: the new *National Security Strategy of the Republic of Croatia*, the *Homeland Security System Act,* and the *Cyber Security Act of the Key Service Operators and Digital Service Providers*. Every new strategy and law initiated new processes that were more focused and directed all actors in building a critical infrastructure protection system towards the common and ultimate goal, which is the establishment of the system.

First Cycle – Year 2013

Significant steps to address critical infrastructure in the Republic of Croatia have started under the influence of the *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection* (*Directive 2008/114/EC*) in 2011 which regulates the issue of European Critical Infrastructures, and by *Directive 2008/114/EC* is determined that the Member States are responsible for establishing a normative framework for the protection of European Critical Infrastructures (Council of the European Union, 2008), which was clearly to many countries an invitation to define the ways of protection of national critical infrastructure as well. Accordingly, the interested professional and scientific public in the Republic of Croatia has increased interest in the subject area through numerous seminars, workshops and conferences on critical infrastructure.

As part of the process of achieving full membership in the European Union, the Republic of Croatia has been obliged to normative arrange and regulate issues of identification, designation and protection of critical European infrastructures by transposing *Directive 2008/114/EC* into its legislation and applying it by the time of accession to full membership. In addition to the abovementioned *Directive 2008/114/EC*, the Republic of Croatia's intentions were to regulate the area of risk management of operations and protection of national critical infrastructures by Act and subordinate legislation, in regards with:

- Critical infrastructure represents the backbone of national and public security as well as sustainable development and progress of key interest, not only for the population/individuals, but also for the overall economy, social activity and the state as a whole;

- Exposure to dangers, those of natural origin, as well as those caused by technical and/or technological processes – including exposure to terrorist activities in the real and cyber space;
- The emphasis on vulnerability of critical infrastructures because the resources of the Republic of Croatia do not allow to develop alternative/redundant systems to a full extent, and the sensitivity increases with the interconnectedness and interdependence of numerous sectors both at the national level as well as with the critical infrastructure sectors of neighboring and other countries;
- The lack of an integral, unified and comprehensive crisis management system.

For the purpose of implementation of *Directive 2008/114/EC* and the regulation of subject area, the Government of the Republic of Croatia on 25 November 2010 adopted a *Decision on the Establishment of the Interagency Working Group to prepare the activities needed to define and determine the National Critical Infrastructure of the Republic of Croatia* which has its work on the development of the *Critical Infrastructure Act* intensify in September 2012. By analyzing the national legislations of the member states of the European Union, working group has decided that the issue of critical infrastructure in the Republic of Croatia should be adequately regulated by the adoption of the Act (Čemerin, 2013).

It was established that the observed practice differs greatly among the European Union countries. For example, the Republic of Italy has decided to regulate only the identification and designation of European critical infrastructures while leaving out normative activity regarding the issues of national critical infrastructures. Most countries have chosen a pragmatic approach and with unique normative framework round up activities related to the identification, designation and protection of European as well as national critical infrastructure. Some countries, such as the Czech Republic and Poland, have made "a step further" and in the necessary integration of the various processes, the activities related to the protection of critical infrastructures have been incorporated into national acts on crisis management. The Republic of Croatia has decided through its legislation to regulate the area of identification, designation and protection of European infrastructure at the same time as national critical infrastructure, which is a comprehensive response to the requirements of the European Commission.

After the public discussion, the Act was submitted to the parliamentary procedure, voted in late April and declared in May 2013. The Act regulates the rights, powers and obligations of the Government of the Republic of Croatia and the central state administration bodies, the powers, rights and obligations of the owner or critical infrastructure manager in identifying, designating and protecting the national critical infrastructure and ensuring their continuous operation. Likewise, the Act regulates the definitions of national and European critical infrastructure, critical infrastructure sectors, critical infrastructure management, making of Risk analysis, Owner/manager security plan, position and role of Security Liaison Officers for critical infrastructure, and that European Critical Infrastructure will be protected by the same measures as the national critical infrastructure. In addition, sensitive and classified information sharing is regulated same as supervision of the implementation of the Act (Government of the Republic of Croatia, 2013a).

The Act laid the foundation for starting multisectoral co-operation process in identifying, designating and protecting national critical infrastructure and cooperation with neighboring countries and European Union bodies in designating and protecting critical European infrastructures on the territory of the Republic of Croatia and other countries. Following the adoption of the normative framework, the preconditions for starting a process of full action to protect, strengthen resilience and reduce negative impacts in the event of the threat to critical infrastructure have been created. In the above mentioned normative framework, the Republic of Croatia has set the assumptions for the establishment of a system that will be responsible for the protection of critical infrastructures, both domestic and European, if marked on our territory.

Pursuant to the *Critical Infrastructure Act*, two more documents have been adopted, which together form the normative framework for the area of achievement of security and strengthening the resilience of critical infrastructures. The first document is: *Decision on Designation the Sectors from which the Central State Administrative Bodies Identify National Critical Infrastructure and Lists of the Order of the Sectors of Critical Infrastructures* which recognizes eleven sectors from which the central state administration bodies (nine competent ministries) can identify national critical infrastructures. These are: 1. Energy, 2. Communication and Information Technology, 3. Transport, 4. Health Care, 5. Water Economy, 6. Food, 7. Finance, 8. Production, Storage and Transport of Dangerous Goods, 9. Public Sector, 10. National Monuments and Values, 11. Science and Education (Government of the Republic of Croatia, 2013d). Second normative document is *Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure* which defines guidelines, criteria and benchmarks for identifying critical infrastructures and risk analysis of critical infrastructure operations, as well as the carriers and their obligations of critical infrastructure business risk analysis (National Protection and Rescue Directorate, 2013). In order to improve and align with international standards, in 2016 it was adopted and applied new *Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure* which are based on the international standard ISO 31000:2009 *Risk management: Principles and Guidelines* (National Protection and Rescue Directorate, 2016), and has outlawed the 2013 Ordinance.

At the stage of its adoption and immediately after its adoption, *Critical Infrastructure Act* has caused many comments on what is needed to be made or what has been omitted in establishing the normative framework. Krunoslav Antoliš (2013) considers that the definition of critical infrastructure in the Act is insufficient because it did not include the term "property" in the concept, where the intellectual capital is especially important as a key factor and the support of the development of the Republic of Croatia, which is a very interesting observation, because intellectual capital is a significant value of every society and it would be important to include it in the definition, but the question is how to articulate it and value it. Ksenija Butorac (2013) has analyzed a number of different methodologies for assessing critical infrastructure business risks and provided a review of the most globally represented assessments. Although such analysis has a large (added) value, unfortunately there was no application in that period. Ivan Pokaz (2013) has emphasized the importance of intelligence support to owners or managers

of critical infrastructures. This is extremely important because if the legislator prescribes to the owners or managers the obligation and the responsibility to protect the critical infrastructure and does not provide them with support in the form of data exchange and the information that is necessary to them and which they cannot attain themselves, then they cannot achieve its fundamental task – to protect its own property, which is a national critical infrastructure.

The importance of this Act is that it represents a systematic act for the critical infrastructure and a central normative point for the observation and application of all activities in this area. This is also valid for the issue of defining the concept and obligations. It was noticeable during that period that many Croatian authors and practitioners used different definitions and mentioned different actors in the process of identifying, designating and protecting critical infrastructures and also used different normative sources of the Republic of Croatia that were adopted before *Critical infrastructure Act*. This was not a good practice and raising awareness meant that the provisions of the Act should become starting point for further discussion and action. The legislator realized that, so when issuing new strategic and normative documents, he conducted the normative alignment and "exclusion" of critical infrastructures from the prescribing of jurisdiction to the documents issued after *Critical infrastructure Act*. As an example can be mention a strategic document named *Disaster Risk Assessment for the Republic of Croatia* adopted in 2015, where the concept of critical infrastructure is only used in the part of the presentation of the consequences of the various risks on their damage or interruption of operations, and the whole framework relies on the concerned Act. Taking that into account, reference to previous documents is no longer relevant.

It is important to outline the levels of competence for the discussion on critical infrastructure. *Critical infrastructure Act* and accompanying decisions and ordinances, has prescribed critical infrastructure protection only for the national level without imposing obligations on local and regional self-government units. It is important to emphasize this for a threefold reason: first, with that, the need and competence to perceive national critical infrastructure at the lower political levels outlined in some earlier strategy papers cease; secondly, units of local and regional self-government in their territory may have national critical infrastructure but they are not responsible for their identification and protection (protection is carried out in coordination with state institutions and owners or critical infrastructure managers); Thirdly, although it is indisputable that local and regional self-government units in their ownership and in their area have local critical infrastructure that is important for their work, human security and business operations, these are not critical national infrastructure.

National Protection and Rescue Directorate (NPRD) – the central state administration body responsible for civil protection activities – has been designated as the coordinating body of the mentioned activities and in general of the entire critical infrastructure protection system. This is understandable given the complementarity of the critical infrastructure protection and civil protection areas, in the context of threat and risk identification, risk assessment and analysis, and risk reduction measures. NPRD is also a national contact point for cooperation with EU member states and the European Commission (Mikac and Cesarec, 2016).

Upon entry into force of the *Critical Infrastructure Act*, NPRD has held consultative meetings with representatives of central government bodies that are subject to the obligations under the Act, regarding: appointment of Security Liaison Officer and its Deputy for each critical infrastructure sector in the area of competence and ensuring the management of critical infrastructure risks and their protection, including – setting sectoral benchmarks for identification and sectoral risk analysis; identification and drafting of critical infrastructure proposals; making sectoral plans for securing operation of critical infrastructure with the provision of delivering goods/services from its scope. There were several working meetings organized where – the principle, context and "spirit" of *Critical infrastructure Act* was interpreted. Meetings are also held on request and by need in the ministries responsible for certain critical infrastructure sectors. Various workshops were carried out as additional support for achieving of the planned implementation activities, but it was noticeable that the underlying obligation was not equally accepted in all competent bodies, where some representatives did not respond to meetings and did not take over the commitments and conclusions of the joint co-ordination of stakeholders involved.

Despite the efforts and initiatives of the National Protection and Rescue Directorate and certain stakeholders from relevant ministries that have recognized the importance of this activity, the initial few years (from 2013 onwards) have been marked by non-harmonized approach and unequal response of all actors in the process. One of the initial challenges was reflected in the lack of political "weight and power" of the system coordinator, the NPRD, which as a state administrative organization represents a body of lower competence than the level of ministries whose implementation activities should prescribe and coordinate. With *Critical infrastructure Act*, ministries as sectoral holders have been set for six months after the adoption of the Act in 2013, to identify the critical infrastructure in their sectors, propose to the Government to designate them by Decision and then together with the owners/managers of these infrastructures to establish and monitor the process of their protection. In the foreseeable period, none of the ministries (nine ministries responsible for the eleven sectors in which it is possible to identify and designate critical infrastructures) hasn't realized what was prescribed, (although there are positive examples of efforts) and precisely for that reason it was not possible to coordinate the establishment of internal processes of the system because the necessary elements for binding the cooperation, practice and exchange of knowledge and experience did not exist.

In the analyzed period, obligations under *Directive 2008/114/EC* have been made in relation to the process of identifying critical European infrastructures. The National Protection and Rescue Directorate has taken the initiative to identify and determine European critical infrastructures on the territory of the Republic of Croatia or the territory of the neighboring European Union member states – Slovenia and Hungary (which are important for the Republic of Croatia) through the bilateral meetings. During bilateral conversation with representatives of the Republic of Slovenia (the Ministry of Defense of the Republic of Slovenia is the national coordinating body for critical infrastructure in the Republic of Slovenia) it has been established that there are no critical infrastructures in the territory of Croatia

or Slovenia which would be significant for both countries. In the consideration of the European critical infrastructure with the Hungary, their representatives (the Ministry of Interior of the Hungary – Disaster Management Directorate is in charge for critical infrastructure in Hungary) have set out as their main priority the identification and designation of their, national critical infrastructures, and only after that, they are ready to discuss on cross-border impacts. It was agreed that following the implementation of the process at the national level, Hungary will establish contact with Croatia for the implementation of the analysis of these impacts (Cesarec, 2017, Mikac and Cesarec, 2019).

The year 2013 was extremely relevant with various content activities related to critical infrastructure issues, but despite all the above mentioned, the ultimate outcome for the first phase of the process of establishing critical infrastructure protection system – the identification of individual facilities, networks or systems as the national critical infrastructure has been left out. Practice has shown (in spite of the existing normative framework, there has not been an initial identification step, and no national critical infrastructure is designated) that long period and an intensive process for establishing such a system is needed. Looking at the positive perspective, although 2013 did not produce concrete results – it has set many things that were the basis for the processes in the coming years. Whether it is the establishment of cooperation between the actors; or certain oversights that are perceived, identified as failures and steps and measures are taken to correct them – that is a capital for the future. In 2013 there were both of such examples.

Second Cycle – Year 2014 to 2015

Encouragements for the continuation of developing the entire process of critical infrastructure protection system and its establishment, was given by process of drafting two strategies: *National Strategy for the Prevention and Countering of Terrorism* and the *National Cyber Security Strategy,* together with the associated Action Plans. Prior to the cross-section why these strategies are significant, it is necessary to draw attention to the three papers (analysis) of national experts who pointed out the essential things in establishing a critical infrastructure protection system.

Anita Perešin and Aleksandar Klaić (2012: 336) have a really good statement that "[critical infrastructure] system protection does not only imply physical protection, but also the protection of data and information systems, i.e. electronic services, linked to a particular critical infrastructure; full application of appropriate information security policies, as well as the protection of cyber space where different types of data are generated and transmitted. Critical information infrastructure, therefore, represents the electronic flow of information and in this sense the cyber space itself is a critical information infrastructure, resulting in the need for a close link between the concepts of critical infrastructure protection and cyber space protection." This stance was not taken into account during the process of drafting *Critical Infrastructure Act* which is in the first place written under the philosophy of protection of physical objects, networks and systems. The authors then say: "It is very important for the establishment of a system of protection [critical infrastructures]

to define a national information security policy" (Perešin and Klaić, 2012: 336). This has been applied during the drafting of *National Cyber Security Strategy,* first such document in the Republic of Croatia. This process is very important because "the security of the cyber space is critical to the security of the critical infrastructure as a whole" (Perešin and Klaić, 2012: 338). The authors conclude that "the protection of the national critical infrastructure cannot be achieved without the proper protection of the cyber space in which the data related to the operation of the critical infrastructure are transmitted and stored" (Perešin and Klaić, 2012: 352). The presented paper shows the inseparable connection between the critical infrastructure elements, its physical and information parts, to which we certainly need to added the third component – people. We have mentioned this paper because, although it was written in 2012, it opened the issues that were solved in the analyzed period from 2014 to 2015.

Another important paper which we want to draw attention to, is related to the importance of the intelligence community support in establishment of effective critical infrastructure protection system and their support to all its stakeholders. Dario Malnar and Nikola Mlinac, employees of the Security and Intelligence Agency of the Republic of Croatia, set out the provisions of *Critical Infrastructure Act* whose implementation requires the engagement of the security and intelligence system – it is a question of analyzing the risks of critical infrastructure operations, developing scenarios of possible threats, developing sectoral benchmarks that include risk assessment, and developing a security plan for owners or managers of critical infrastructures (Malnar and Mlinac, 2014). This is very important because we are aware of the need for co-operation between the National Protection and Rescue Directorate and the intelligence community that was expressed by Security and Intelligence Agency staff in academia scope (e.g. through papers), while real co-operation has not occurred in the required profile over the years in which *Critical Infrastructure Act* was adopted. The authors then report the activities that the intelligence system implements, and are linked to processes of this research interest. They state that "the security intelligence system operates through data collection and strategically-analytically through the evaluation and processing of available data, both in the area of strategic documents preparation and threat and risk assessment, as well as in analyzing processes of great importance for the protection of critical infrastructure." All which is here said is necessary, but the question is how much has been implemented in practice? The authors themselves ask the same questions: "Key questions are the ways in which the security intelligence component can be most effectively used in the protection of critical national infrastructure, questions related to the processes of defining critical infrastructure protection requirements for security intelligence services and the correlation of critical infrastructure system security needs with the potentials of the intelligence community" (Malnar and Mlinac, 2014: 1013). Everything stated, shows that within various security sector organizations we are aware of the need for greater co-operation and coordination, but it is build up too slow in relation to the existing situation. The authors emphasize that "critical infrastructure protection, despite the construction of national protection system and efforts to centralize the activities, is still largely fragmented activity, sector-defined through the scopes of

various ministries and other state bodies. Such dispersion of protection and the particularization of facilities makes it difficult to concentrate intelligence efforts and negatively affect the effectiveness of the action" (Malnar and Mlinac, 2014: 1013).

As a third paper, it need to be highlight the opinion of Ivan Pokaz and Uta Perčić who have noticed a few key things about why the system is not set in motion and what needs to be changed. They correctly set the assumption of the problem in the absence of a formalized system of national security, as well as for the consideration of areas and activities within the critical infrastructure concept that opens up many uncertainties. They noticed how *Critical Infrastructure Act* did not give priority to the threats of terrorism and in their opinion it supposed to (Pokaz and Perčić, 2014: 1137). The authors of the Act didn't directly mention terrorism, they have opted for a more neutral expression (term) in Article 6: "The central state administration body, within whose competence are protection and rescue tasks, in cooperation with competent central state administration bodies in which scope certain critical infrastructure is, regularly monitors, assesses the threats and proposes operational and other measures to assess the criticality and the need for proposing measures for the management and protection of critical infrastructure" (Government of the Republic of Croatia, 2013a). This formulation leaves ambiguity because "it is not clear which threats are in mind", ... NPRD "has a priority task of protection and rescue in the event of major accidents and disasters ... but not the task of assessing the threat posed by intentional, hostile action of man or man-made entity (terrorism, organized crime, cybercrime, the activities of foreign intelligence agencies and other" (Pokaz and Perčić, 2014: 1138). The assumption is that the creators of such expression in the text of the Act have been guided by the premise that NPRD by that point has failed to establish an adequate level of cooperation with security sector agencies (primarily with the intelligence community) to use their knowledge and products for the purpose of assessing the threats and coordination of others actors within the system. More logical explanation is that it was not payed enough attention on the details during drafting of the Act, while general idea here is that is structural issue. This is also confirmed by Pokaz and Perčić (2014: 1137) by stating that the Act is "an indication of insufficient understanding of security risks management issues and terminology in that area." It is therefore necessary to include all progressive forces from the state, civil, private and academic world in all processes of social activity in order to jointly develop better solutions for the well-being all of us.

In 2015 two significant, previously mentioned, security strategies were adopted – the *National Strategy for Prevention and Countering Terrorism* and the *National Cyber Security Strategy*, together with the associated Action Plans. Both are significant because the area of critical infrastructure within these is strongly recognized and represented. This is largely the result of the intensive advocacy of the National Protection and Rescue Directorate (not lessening the value of contributions of some colleagues from other state administration bodies who are all the time present, active and helping the process become so visible) during their participation in working groups for developing mentioned strategies, as they have seen the possibility to actualize this area and make it visible by all stakeholders

in the political and security sector (as they at the highest level have the ability to restart the process).

National Strategy for Prevention and Countering Terrorism recognizes the terrorist threat and potential attack on national critical infrastructure whose interruption in operation or delivery of supplies, goods or services may have serious consequences on national security, the health and lives of people, property and the environment, security and economic stability and continuous functioning of government. The activities required to protect the critical infrastructure from terrorism are outlined through the following measures: "a. development and strengthening of national capabilities for the protection of people and property; b. designation and timely activation of a special regime for the protection of locations and structures of particular importance for defense; c. protection of diplomatic, consular and other representative offices of the Republic of Croatia abroad; d. informing Croatian citizens and legal persons about the level of terrorist threats in the countries in which they travel or operate; e. protection of diplomatic, consular and other foreign representations on the territory of the Republic of Croatia; f. adapting the existing concepts in the area of national security and the legal framework for the establishment of emergency and crisis situations management systems, and thus in the case of terrorist activities; g. strengthening the protection and surveillance system of the state border; h. reinforcement of armaments and disarmament control, as well as storing weapons, explosives and other means that can be used to commit a terrorist attack; i. strengthening the supervision of transport and use of dual-use goods; j. establishment of critical infrastructure protection system, with respect and application of existing sector-specific measures of protection, plans and competencies; k. establishment of a system of continuation of critical business infrastructure operations; l. strengthening the civil protection system; m. strengthening surveillance over possible cyberattacks" (Government of the Republic of Croatia, 2015b: paragraph 23). It is clear that the authors of the Strategy described the concept of critical infrastructures with all the necessary activities and the development of support functions much more broadly than the immediate protection, hoping to put forth a positive reaction and more attention to the organization of critical infrastructure system. But this did not happen as expected.

The *National Cyber Security Strategy* and *Action Plan for Implementation of the National Cyber Security Strategy* highlighted much more the area of critical infrastructure than all the national strategies, assessments and plans so far. It was primarily observed through critical communication and information infrastructures that were defined as communication and information systems whose functioning disorder would have significantly disrupted the work of individual or several identified national critical infrastructures. The Strategy has a great space dedicated to critical communication and information infrastructure in conjunction with the management of cyber crises. In general, the Strategy strongly emphasizes the importance of the *Critical Infrastructure Act* and the need for putting it in practice. Specifically, Strategy brings a total of five goals that needs to be realized to protect critical communication and information infrastructure and effectively manage cyber crises:

1. Establishing criteria for critical communication and information infrastructure recognition;
2. Determining the binding security measures applied by the owners/managers of designated critical communication and information infrastructure;
3. Strengthen prevention and protection through risk management;
4. Strengthen public-private partnerships and technical coordination in the processing of computer security incidents;
5. Establish capacities for an effective response to a threat that may result in a cyber crisis (Government of the Republic of Croatia 2015a: item 5.2.).

The Strategy states the need to identify critical communication and information infrastructure and all those procedures that two years ago prescribed *Critical infrastructure Act*, which have not been implemented. The problem is that the state bodies should carry out that process, but they did not, and it raises the question which image/message State are sending to private owners or managers of critical infrastructures, to the wider public, to the European Commission? All five measures provide the excellent guidance what needs to be done, and it is important to specifically outline Objective 3 "Strengthening prevention and protection through risk management", proposed structure what sectoral risk assessment includes: identification of critical functions (services, data, networks, etc.); identification of threats; threats, vulnerabilities and consequences assessment; risk analysis and prioritization; determining acceptable risk and risk management. The above-mentioned (with the prior knowledge that the Security Intelligence System has the capacity and ability to assist in making such assessments) leads us to the conclusion that all elements and stakeholders need to initially make a sectoral assessment, followed by a sectoral plan for ensuring critical infrastructure operations – which will all together give a framework for forming sectoral policies and opening up constructive co-operation with key stakeholders in the sectoral processes.

Furthermore, it should be noted that there is no specialized and comprehensive program in a higher education institution in the Republic of Croatia where everyone involved in critical infrastructure related activities could be educated and acquire the basic knowledge necessary for a better implementation of tasks and responsibilities in the field of identification, protection and strengthening of critical infrastructure resilience. In search of an *ad hoc* solution in providing basic and equal understanding among all stakeholders (from NPRD representatives to Security Liaison Officers and their deputies from nine ministries) and harmonizing the expectations and knowledge of these experts, an initial course called "Business Critical Infrastructure Risk Analysis", 2014 was conducted. There was also an advanced course in 2015 called "Assessing risk assessment and optimal risk management in accordance with ISO 31000 and IEC 31010". Both seminars were commissioned and funded by NPRD, and the University of Applied Sciences Velika Gorica with external associates has conducted them. Thereafter, no education or training was carried out and none of the higher education institutions has launched a specialized program designed to educate staff working on critical infrastructure protection.

Therefore, it is necessary for the future, to plan professional (expert) training as well as education for critical infrastructure owners/managers, so that all stakeholders have initial and equal knowledge of the importance, interdependence and ways of functioning of the concept of critical infrastructure protection. To achieve that, it is necessary to provide financial resources, plans and training programs for stakeholders in the critical infrastructure risk management system – to increase knowledge and competences and as much as possible to include the scientific community and to prescribe the obligation of education. In all countries where the critical infrastructure protection system is highly developed, great attention is paid to education, so Republic of Croatia also needs to develop a model for training of all key players who have their roles and responsibilities within critical infrastructure protection system.

Third cycle – 2016 – 2018

Taking into account the fact that the creation of an adequate system of critical infrastructure protection requires continuous work and investment in the development of the area, it is necessary to establish the predispositions for a strong normative arrangement with coordinated implementation of activities in order to ensure harmonized implementation of regulations, measures and procedures in the protection of critical infrastructures. Accordingly, the National Protection and Rescue Directorate as the competent authority has produced in 2016 *Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure* (National Protection and Rescue Directorate, 2016), in 2017 bylaw on *Amendments to the Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure* (National Protection and Rescue Directorate, 2017), and in 2018 it started revising the *Critical Infrastructure Act* itself. This can provide a good foundation for the establishment of a system that will ensure the realization of all unsuccessful efforts at the national level, which would certainly strengthen the position of the Republic of Croatia in the international field, in accordance with the goals and objectives set by the European Union for the Member States.

The overall challenges so far, have been actualized again in 2017 by drafting two important documents within the area of national security that introduce critical infrastructure into a list of considerations and priorities: the *National Security Strategy of the Republic of Croatia* and the *Homeland Security System Act*. The Strategy, among other things, brings nine strategic goals of the Republic of Croatia that represent the concrete implementation of national security policy. The strategic goal of "Reaching the highest level of security and protection of the population and critical infrastructure" is linked to and derives from (one of the four fundamental national interests) of national interest "Security of the population, territorial integrity and sovereignty of the Republic of Croatia". Within that strategic goal, great attention is devoted to critical infrastructure with the initial stipulation that for a safe society it is necessary to protect life, rescue people and goods and protect critical infrastructures. Subsequently, several important sections are devoted to the activities expected from all stakeholders in the formulation of security policies. "Critical infrastructure protection will focus on the prevention,

elimination or mitigation of risks that can cause critical infrastructure vulnerabilities and enhance their resilience. The management and control system for some critical infrastructures needs to be continuously upgraded and improved, with applied best experience available in other countries in this area. Data exchange models will be developed between state bodies and agencies and critical infrastructure managers in public and private ownership for timely recognition of potential security threats and risks" (Croatian Parliament, 2017a: national interest under mark A)

"By developing documents which are defining the policy and methodologies of critical infrastructure management and limited national goods, the Republic of Croatia will clearly identify which parts of it should remain in the state's majority ownership, thus preventing the endangerment of vital functions important for the state and the population in cases of business instability. Strengthening the national critical infrastructure resilience in relation to modern security challenges and risks, requires simultaneous maintenance and protection of national critical civil capabilities that will support the overall capabilities of a coordinated comprehensive public and private sector, primarily private security sector. These efforts will also be aligned with allies, international organizations and partners. Civilian preparedness, which is entirely national responsibility, is the backbone of national resilience" (Croatian Parliament, 2017a: national interest under mark A).

Most of the above mentioned provisions have been defined earlier, as well as many times stated by expert and academic community in numerous discussions on critical infrastructure issues. What is important to emphasize, although this is not an absolute novelty, it is remarkably significant that it is stated in the document of this level – necessity to determine which parts of the critical infrastructure must remain in the state's majority ownership, so it doesn't happen that we invest the maximum effort to prevent and protect certain critical infrastructure, and then someone who is potentially unbefitting, legitimately buys it on the stock market and takes over majority of stakes in the company.

The *National Security Strategy of the Republic of Croatia* is a fundamental strategic document that sets out policies and instruments for achieving visions and national interests and achieving security conditions that will enable a balanced and continuous development of the state and society. It is very important from the discourse of this research that the concept of critical infrastructure is strongly represented in the Strategy. In order for the Strategy to be operationalized in practice in the part related to the establishment of the Homeland Security System and its related management of security risks, crisis and critical infrastructure management – the *Homeland Security System Act* was adopted.

The *Homeland Security System Act* does not change the competencies of state bodies or their responsibilities under other laws but links them to the coordinative action related to the management of security risks and actions in crisis. This is an Act that has been urgently needed in the Republic of Croatia, it is extremely important and it is very significant that critical infrastructure is heavily represented in it. The introductory part of the Act among the six key provisions also sets out the intent of ensuring a harmonized implementation of regulations that define the security measures and procedures of importance for national security, and in particular the

protection of critical infrastructures. On the basis of the Act, the Coordination for the Homeland Security System was established as the inter-authority body responsible for harmonizing and coordinating the work of the Homeland Security System (Croatian Parliament, 2017b). Coordination was established and then adopted the Annual Work Plan of Coordination for the Homeland Security System of the Republic of Croatia in 2018 and 2019, where the need to identify and designate critical national infrastructures was re-updated as well as the amendments to the *Critical Infrastructure Act*.

With regard to the establishment of cyber security, based on *National Cyber Security Strategy* of 2015, in 2018 *Cyber Security Act of the Key Service Operators and Digital Service Providers* was adopted, which regulates the rights and obligations of the stakeholders of the system concerned and within the criteria are adopted, set out in Annex 1. *A list of key services with criteria and thresholds to determine the importance of the negative impact of the incident* (Croatian Parliament, 2018). With this Act, the *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 (NIS Directive)* has been transposed into national legislation. Upon the adoption of the Act, the procedure for identification and prescribed measures for the protection of communication and information infrastructure was established in the Republic of Croatia, and certain Key Service Operators and Digital Service Providers were identified within the legal deadline. The mentioned Act and the processes conducted under its framework are in this initial stage a positive example of how things needs to be done. The experience of the processes that took place under the aegis of the *Critical Infrastructure Act* has certainly contributed to that. For the period in front of us (and it is a short-term consideration of the year or two) it is left to see how processes within these two legislative frameworks will be harmonized, where there will be challenges in overlapping and how it will they be resolved.

To conclude, for this part, it should be noted that in the observed and analyzed period the overall efforts of the past years since the adoption of the *Critical Infrastructures Act*, bylaws, new strategies, numerous activities and workshops – have resulted in the identification of a number of critical infrastructures in particular sectors – just some of them, and not in all. This is an important step forward in further steps towards setting up critical infrastructure protection system. The exact number of identified critical national infrastructures is confidential. On the other hand, there is publicly available information accordingly to the *The Cyber Security Act of the Key Service Operators and Digital Service Providers* that we currently have identified and designated 98 Key Service Operators and Digital Service Providers in the Republic of Croatia.

5.3. Structural Challenges in Establishing a Critical Infrastructure Protection System

Since the area of critical infrastructure is a highly dynamic arena that involves different actors, their policies, needs and perceiving things; belongs to national security; makes central part of many events around the world and a medium for

the realization of various projects – the process of establishing a system of critical infrastructure protection in the Republic of Croatia was not implemented in the early years following the adoption of the *Critical Infrastructure Act*. Although the system has not been established until the writing of this analysis, many positive steps have been taken on this path, but there is still a regret about missed time and opportunities.

It shows that the overall process of taking over the *Acquis communautaire* in the field of critical infrastructure has not been sufficiently well prepared and implemented, yet the goal was fulfillment of the norm for accession to the Union's full membership. The main reason for this is the lack of a strategic vision at the highest political level to implement this process as well as to "allow" lower subordinates to fulfill their obligations under the Act. As a result, the numerous negative comments on the account of the National Protection and Rescue Directorate has been made, such as it's not doing the job for which is responsible as the coordinating body of the process related to critical infrastructure in the Republic of Croatia. Although the NPRD had certain omissions in everything before mentioned, the negative comments were mostly unfounded because NPRD could not begin to establish and build a system of critical infrastructure protection when the ministries which had to be coordinated "did not agree" to be coordinated. The National Protection and Rescue Directorate, from its establishment, is also followed by „mantra" of unrealized organization in its legal powers and capacities, partly because it was not enabled for them to achieve that (insufficient finance, staffing, no clear guidelines, conflicts of jurisdiction (the most obvious example in segment of firefighting management) and no appreciation of various ministries in the realization of legal obligations and tasks), and partly by their own wrong policies and practices. So, NPRD has become a "favorite target for criticism" for many actors.

Particularly important is to highlight few things so there can be no impression on any reader that significant objects, networks or systems in the Republic of Croatia are unprotected or with a low level of protection. Critical infrastructure is protected even without the existence of a system. Many complementary processes are carried out in accordance with other legal bases and the most important critical infrastructure in the Republic of Croatia is protected by a high level of protection. Only they are not called (officially named) „national critical infrastructure" in accordance with the *Critical Infrastructure Act*.

The first such process was launched in 1999 by adopting the *Ordinance on Criteria for the Designation and Protection of Objects of Special Importance for the Defense of the Country* in accordance with the *Defense Act* (Official Gazette 74/93, 57/96). Through this process the criteria for the designation of military and other objects of particular importance to the defense of the country have been developed, a methodology has been developed for the assessment of threats and the plan for the protection of military and other objects, the specified objects and their catalogue have been established, general and special measures of protection of those facilities as well as many other activities. The process is established, well-functioning and effective. There is a great similarity, and in some cases identically of the provisions set forth with those of the *Critical Infrastructure Act* and the related sub-legal act. It should be noted here that, although these processes have been

complementary, their harmonization and common approach to the owners or managers of certain objects of particular importance to the defense of the country did not happen. This fact is particularly emphasized by experts working in these facilities – as in a large number of cases they are the same objects (because there are no others), which are, through a system coordinated by the Ministry of Defense of the Republic of Croatia, designated as objects of particular importance for the defense of the country and they will most likely also be designated as a national critical infrastructure within the future system coordinated by the National Protection and Rescue Directorate. What is important here is that there is no necessary level of coordination between the Ministry of Defense of the Republic of Croatia and the National Protection and Rescue Directorate to harmonize the processes.

The next instance is about aligning and ensuring the complementarity of the Republic of Croatia with regard to cooperation with the NATO Alliance in the field of crisis management. In February 2014, the Government of the Republic of Croatia adopted *Decision on Determining National Implementation Coordinators of Crisis Response Measures of the North Atlantic Treaty Organization in the Republic of Croatia and their Responsibilities* (Government of the Republic of Croatia, 2014). In accordance with the Decision, the operational document for the implementation of crisis response measures is *NATO Crisis Response System Manual*. Significance is that in the Manual, among all others, the activities and actions related to the critical infrastructure protection are prescribed, and the coordinator of the whole process is the Ministry of Defense. After the Government Decision, followed the process of designating the activity holder for each of the critical infrastructure protection measures outlined in the Manual. After the designation of the activity bearer, scenarios for each of the measures were drawn up and merged into the document prepared by the Ministry of Defense and reported to the Government of the Republic of Croatia. Here we have an absolutely different situation regarding the cooperation between the Ministry of Defense and the National Protection and Rescue Directorate. In the process linked to use of *NATO Crisis Response System Manual,* Ministry of Defense and the National Protection and Rescue Directorate cooperate very well and coordinated, and the logical question is why does this not work in the previous case?

These examples illustrate different practices and solutions – inadequate coordination in the first process and joint collaboration in the second. After this overview, it is a rightful thing to ask – why the state does not coordinate its key security processes? Additionally, if the Ministry of Defense and the National Protection and Rescue Directorate cannot align themselves, then the question is who coordinates them and in which quality? Such situations are an indicator that the Republic of Croatia has a lot of room to improve security sector management, coordination of key processes and actors, and greater use of research and science in all of these activities.

The most frequent discussion on the reasons why the critical infrastructure protection system in the Republic of Croatia is not established leads to the facts what the NPRD has or has not done or should have done. Here it is not a case to defend of National Protection and Rescue Directorate because of its limitations and

omissions that are actually grounded in the relationship of power within the state administration system, the designation of strategic priorities (both at the state level and the NPRD itself) and to small number of personnel assigned to deal with this topic (as well as their competencies). In this section is need to emphasize some challenges that prevent the establishment and then the effective development of critical infrastructure protection system. There are presented to point out the things that needs to be changed from the roots.

One of the features of the discussion is too much commitment to critical infrastructure protection *per se* and neglection other essential components that make the system and its components long-term functional. There are interest groups that have focus primarily on the protection of critical infrastructure, which is understandable because they operate on market principles and have their own interest. But the interest of the state is to devote more attention to the overall concept and to clearly define the communication policy in this matter. In this policy, it is necessary to clearly and unambiguously present how the state sees management in this area through the application of all measures and activities of comprehensive action. Responding to the question how to protect a national critical infrastructure from sources of threats, we should start from the interpretation of potential sources of endangerment – natural, technical-technological nature, and acts committed and motivated by people. In the analysis of potential threats we have to perceive all the risks in the expanse, starting from where the object, network or system is located; what could endanger it; to human – induced threats, whether from in – house employees who for any reason wants to apply damage or the threats from external attackers. We will adequately protect critical infrastructure, but also the entire country, by diversifying as far as possible the sources, areas and sectors we are heavily dependent on. Critical infrastructure will be best protected if its built in as less possible risky areas of flood and earthquake, according to the rules of the profession and with the use of quality materials and systems, respecting all construction and maintenance standards. The next step is to draft the complete supporting documentation and obtain the knowledge of the processes themselves to avoid any delays and possible domino effects if a system fails or malfunction occurs within a particular facility or key infrastructure. Then, we talk about the resilience of the system itself, its robustness and high functionality. After that, the question is whether the company has made all the necessary assessments, analyzes and plans required by other acts because the issue of critical infrastructure is just an upgrade to everything previously done. It would certainly be a good thing for the company to harmonize and/or improve its business to one of the international standards for business, quality management, crisis management and/or emergency management. It is also important whether they have a crisis plan, a crisis communication plan, do they conduct internal exercises, are they linked with urgent services, and such. So there is a whole range of necessary activities before we begin to talk about technical and physical protection, and the co-operation, coordination and exchange of knowledge and experience are of crucial significance (Mikac, 2017).

When we are talking about the implementation of *Directive 2008/114/EC* in Croatian legislation, time has shown that it was too optimistic to open up the

possibility of identifying and designating critical infrastructures in eleven sectors. On the other hand, it was most likely a pragmatic solution when the *Critical Infrastructure Act* with accompanying documents has already been written and the area was widely considered, to include all major sectors. *Directive 2008/114/EC* has obliged all Member States to consider two sectors: energy and transport. With time, it is clear that the initial idea as well as the design and structure of the future system in the Republic of Croatia was overoptimistic. Yet activity can still be directed towards an acceptable solution within the scope of the possibilities. It's just about having a strategic management capability. It is useful in the given circumstances to redirect existing efforts in present extent and to focus on the transport and energy sectors in identification and designation of the first critical national infrastructures in order to be in the course of what is of the utmost interest to the European Commission. With that being done, we could cooperate with other EU countries that have gone a step further from us in this process. In parallel, we need to work on other sectors to get the overall situational picture and build the system. The level of protection will depend on the prioritization of each sector according to sectoral and cross-sectoral criteria: "what is more and less important to us". Procedures will be determined by security plans that will also have to be prepared. If we get a large number of sectoral decisions on identified critical infrastructures, there will be a blockage of system functioning even before it starts operating in its functionality. In the number of specific sectoral critical infrastructures, there were mentioning of one hundred facilities that the sectors could potentially suggest as critical infrastructure. Consequently, the question is what is really critical in the Republic of Croatia and without what we cannot function because all that has an alternative is not critical. For comparison we can take the Republic of Slovenia, which has successfully completed the identification process and has a total of eight sectors where they have identified at least one critical infrastructure within each, and for the whole country, they have designated less than 60 critical infrastructures.

Thereafter, the question arises how come some ministries needed several years to fulfill their obligations, and some of them even after five years did not identify at least one critical infrastructure in their sector? Thereby it is valid and absolutely legitimate to decide that we do not have any infrastructure that could be considered as critical in the particular sector, but not even such decisions have been made. Why is the situation like this, there is no concrete answer, because it is a combination of several different factors. We can say that this process is not very interesting to the highest level of government, so that is why there has not been a critical infrastructure designation in some sectors, if not in all of them. The other thing is that so far, much has been done on the development of sectoral measures and the "current state analysis" within the sector, but the "last step" is missing, which is a proposal to the Government of the Republic of Croatia to designate identified facilities, networks and/or systems as national critical infrastructure. Part of the answer lies also in the fact that in the state administration system we do not have a job position of the Security Liaison Officer, which is a key point and position that should/must „push the process" as the fulfillment of its responsibilities. Whether it is necessary to prescribe such job position is a matter of perspective,

but it is undeniable that its existence would facilitate the processes that must be carried out. At the same time, we come to the question whether the current Security Liaison Officer are adequately positioned within their own sectors and whether they can acquaint and draw attention of their superiors to the importance of this process. The same problems have been identified with the hierarchical positioning of Information Security Advisers (in accordance with the *Information Security Act*) in some state bodies. As this two positions are complementary in tasks and responsibilities, it would be necessary to unify them, to prescribe competencies and to form a department in which personnel in charge of the subject areas in larger bodies would work jointly, while in smaller bodies or bodies with a lower coverage of competencies (such as the Ministry of Culture) that should be the task of the same person.

After this, we come to consideration of the fact that there is no structurally prepared basis for application of such important area in the Republic of Croatia. Why is it important? Because all the highly developed countries invest a lot of time, energy and financial resources into the development of concepts, systems and knowledge of critical infrastructures. The European Commission has given a lot of attention to this area, finances numerous activities and projects. Big companies are increasingly seeking specific knowledge and services to strengthen resilience and protect their critical infrastructure. If we want to keep up with all of them, we have to invest more. Structurally, the entire state administration has not prepared the basic assumptions for the implementation of critical infrastructure protection – there is no sufficient number of personnel capable of coordinating the entire process; no required framework and programs for training the personnel who need to work on critical infrastructure issues; no prescribed qualifications of the persons who need to be employed on these jobs and there is no job positions for critical infrastructure Security Liaison Officers but the responsibility is given non-selectively and sporadically although this is a full-time job. Also, there is no education of inspectors that should supervise the implementation and they are completely out of the content of subject matter. In addition, the Croatian model of public-private partnership is legally limited to investments in construction and maintenance of facilities and is not even slightly tailored to the needs of critical infrastructure area. It is also necessary to change that.

Another important thing we cannot miss out, is the relationship with owners or managers of critical infrastructures. It is not a partnership but relationship where state is acting as higher authority, not involving owners/managers to be the part of discussion on the models of governance and mutual exchange of information, and from the level of the state, they are mostly dealt with the norms and what they have to fulfill without providing them an adequate level of support. The question is why would a private owner accept the decision that it was designated as national critical infrastructure? Most often they will get such decision, without previously consulted and such approach is not good. With each owner or manager, it is necessary to talk about the benefits and disadvantages, and if the state prescribes a higher level of protection where they must invest from its own profits – inform them in which way they may have certain benefits in such partnership/relationship. The state needs to offer adequate benefits for that companies, and for best of them use economic

diplomacy and help them emerge in new markets, and can also place them on a list of companies that the state guarantees for doing business with, for example, with the NATO Alliance – because without the support of the state, companies cannot work independently with NATO. The state can upon the existing examples (from other countries) set up a fund for investments in critical infrastructure protection, where different fundraising models exists, and provide investment in a higher level of protection that the state prescribes for certain infrastructures. There is a lot of international positive practice, so some of these good examples should be applied to the Republic of Croatia.

Chapter conclusion

All identified challenges in the development of critical infrastructure protection system in the Republic of Croatia from previous experience can be consisted to several key points: inadequate and unsuitable communication and cooperation of critical infrastructure Security Liaison Officers with decision-makers in central government bodies at all levels; insufficient cooperation of central state administration bodies with competent agencies and professional associations; insufficient education of stakeholders; lack of regulation; the responsible state bodies do not have the necessary tools (software) in the area of risk management of critical infrastructures; the lack of scientific-research activities in this area.

All of these challenges are transformed into recognized needs in terms of the actions necessary to create an adequate system of critical infrastructure protection at the national level. According to the analyses of needs for establishment of a high-quality critical infrastructure protection system, which are done so far, certain recommendations can be given. In the phase of designating the critical infrastructure that is forthcoming after the identification, great attention should be directed on the criterion of criticality and national importance of the infrastructure so the aspiration of certain sectors to imply their importance would not administratively burden the system by identifying too many infrastructures whose criticality is insufficient. This also slows down the process of designating the critical infrastructure carried out by the Government by adopting a Decision on critical infrastructure designation. It is necessary after the designation to have the prioritization because all critical infrastructure do not require (and even not all of components within) equal level of protection and not all have the same importance. Concerning further activities and phases in the realization of critical infrastructure protection, it is necessary to introduce into the system appropriate internationally recognized standards as well, (such as *International Standard ISO 31000: 2009 Risk Management: Principles and Guidelines*) which are in function of risk assessment and business continuity of critical infrastructure.

Concerning stakeholder cooperation, the key component is the public-private partnership and the establishment of high-quality cooperation. The private sector that is most often the owner and the critical infrastructure manager (such as the Croatian Telecom in the Information and Telecommunication sector) has the responsibility to protect the infrastructure that is important to the functionality of the entire society, and this cannot be done efficiently and without greater cost

if there is no cooperation with public institutions. Such a relationship creates a number of open issues, such as: developing common procedures, exchanging the previously mentioned sensitive data to which relates building of trust, exchange of knowledge and experiences. That is why, in the Republic of Croatia, it is necessary to establish an acceptable common model of cooperation in this area with clearly defined mutual rights and obligations.

The development of the model and, in general, all components addressing critical infrastructure protection system should be directed to the special body which would in the fulfillment of their tasks, have institutional power and influence on all system stakeholders. In many countries there are good examples (such as the United States, Great Britain, Romania) for the successful formation of such bodies that are called *Critical Infrastructure Protection Centers*. By analyzing their activities it is possible to adjust them and accordingly form that kind of Center in the Republic of Croatia as well.

Additionally, efforts should be made to improve the system and to conceptualize methods for enhancing awareness on the importance of critical infrastructures – for the wellbeing of the population, the functioning of the economy, public and national security and raising awareness of their interdependence, importance of their protection and risk management, as well as risks that potentially endanger it. Critical infrastructure protection is the responsibility and obligation of the entire society, so a consensus is needed at national level in terms of the national critical infrastructure protection program, which is difficult to achieve without political support to ensure the development and progress of the process. In 2017, the *National Security Strategy* and the *Homeland Security System Act* were adopted, within the protection of critical infrastructures was identified as one of the strategic goals of the Republic of Croatia which changes the state of affairs in the context of recognizing the importance of the concept of critical infrastructure protection. With that, the possibility of realizing all the efforts we have made so far, increases to the option of much better quality system than the one we had assumed to be able to establish.

About authors

Marina Mitrevska is a Full Professor at the Institute for Security, Defence and Peace at the Faculty of Philosophy, University of Ss. Cyril and Methodious in Skopje, Republic of North Macedonia. She is Head of the third cycle doctoral studies in security, defence and peace. She is a member of the Accreditation and Evluation Board of Higher Education in the Republic of North Macedonia. She is Editor-in-Chief of the international scientific journal Contemporary Macedonian Defence. Her field of scientific research is security, diplomacy, peacekeeping operations and crisis management. She is actively engaged in researching and publishing scientific papers and books in the field of security. She is the author of eleven books and more than a hundred scientific papers.

E-mail: marinamitrevska@yahoo.com

Toni Mileski is a Macedonian full professor and researcher in the field of political geography and geopolitics, environmental security, energy security and migration and conflicts. He is an employee of the Ss. Cyril and Methodius University, Faculty of Philosophy – Department of security, defence and peace. Professor Mileski has taken participation in several scientific and research project. In October 2012 he participated in the International Visitor Leadership Program organized by US Embassy. Program held in Washington, New York and Boston, USA. Recently, he is second year consequently programme coordinator of the two projects developed together with Brandenburg University of Technology in Cottbus – Germany and DAAD Foundation. He is the author of six books, several books chapters and more than an eighty scientific papers.

E-mail: toni@fzf.ukim.edu.mk

Robert Mikac is Assistant Professor at the Faculty of Political Science of the University of Zagreb in the area of Social Sciences, Field of Political Science, Subfield International Relations and National Security. Areas of his interest and expertise are: International Relations; International and National Security; Security Management; Crisis and Disaster Management; Civil Protection; Afghanistan; Privatization of Security, Critical Infrastructure Protection and Resilience; Migrations and Security. Unitl now he published three books (the first on Afghanistan, the second on Privatization of Security, the third on Critical Infrastructure Protection) and about forty scientific and expert papers. At the previous workplace in National Protection and Rescue Directorate was in charge of affairs related to critical infrastructure, and from 2012 till 2015 the national point of contact for critical infrastructure.

E-mail: robert.mikac@yahoo.com

Richard Larkin is the former Director of Emergency Management for the City of Saint Paul, Minnesota, USA. He has over 30 years' experience in Public Safety as an Emergency Medical Technician/Paramedic, Firefighter, and Emergency Management practitioner in the 16th largest metropolitan area in the United States. He has been involved in Emergency Management (Civil Protection/Crisis Management) program review and support activities in Hong Kong, PRC; Peru, Republic of Croatia and 3 of the British Overseas Territories in the Caribbean. His areas of his interest and expertise are: Emergency Management and Homeland Security Program Administration, Crisis and Disaster Management; Civil Protection; Critical Infrastructure Protection and Resilience; National Standards and Accreditation of Emergency Management and Business Continuity programs, Emergency Planning and Preparedness, Incident Management and Emergency Response. He is a member of the international Institute for Security Policy and a past Chairperson for an International Emergency Management Standard Development Organization (EMAP). He is also a contributing author to 3 peer-reviewed textbooks on Critical Infrastructure Protection and Resilience.

E-mail: rjlarkin103@gmail.com

Matthew Vatter is a retired Senior Army officer from Minnesota National Guard. During his assignment to the Minnesota National Guard, he held numerous leadership positions culminating as the Director of Strategic Plans and Policy. In this capacity he led the MN National Guard Contingency Operations program which focused on Military Support to Civil Authority during National emergencies and national disasters. His team wrote and exercised the plans that provide military resources to civilian authorities and established command authority and relationship development among local, state and tribal emergency response agencies. He oversaw the state partnership program with the country of Croatia assisting Croatia with the development of various National security programs and policies to include crisis response, critical infrastructure protection and cyber defense training along with traditional military inter-operability. He is a graduate of the United States Army War College and the Universities of Minnesota and Wisconsin. He holds an undergraduate degree in earth science education and masters of science degrees in strategy and security technologies. He has contributed to academic texts on critical infrastructure protection and written academic papers on energy resiliency. He currently serves the state of Minnesota as an Assistant Commissioner for the Department of Commerce where he leads a team 58 consumer service agents and professional investigators. He frequently lectures on cyber security for small business and the shared responsibility of government and private sector on security and resiliency.

E-mail: mattvatter@gmail.com