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 2

CRITICAL INFRASTRUCTURE PROTECTION IN THE EUROPEAN UNION

CHAPTER 2

Critical Infrastructure Protection in the European Union[3]

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

While some countries like Great Britain, Sweden, Germany, the Netherlands and France are advanced in the development of national policies of critical infrastructure protection, the European Union is still seeking its place and role in this area. From the European Union institutions, the European Commission is most active and seeks to promote the importance of this topic, to ensure cooperation between Member States, to accelerate the exchange of knowledge and experience and to guide the Member States in their efforts to develop the area of strengthening resilience and critical infrastructure protection. Challenges at the European Union level are multidimensional and are under time pressure, because as Haemmerli and Renda (2010) remarkably noticed, it is necessary to harmonize Europe at "several tracks", to harmonize various policies and in all of that to find and create own identity in this area. Therefore, the Union is trying at an accelerated pace to develop its own recognisability and set standards to be followed by all Member States.

The chapter is set in a timeline from the consideration of the individual activities of certain states and their development of the area of critical infrastructure protection to the activities of the European Union and the efforts of binding states, processes, critical infrastructures and experts. The main feature of these activities, both in states and at the Union level, is in initial consideration – normative arrangement, then a certain (expected) delay in implementation caused by numerous factors, after that the continuation of development (in phases) primarily dependent on the imagination and commitment of individuals (we consider them as key factors) within organizations, which have enabled with their ideas and endeavours continuation of the development of certain activities.

It is important to point out that there is an important difference between the concept of critical infrastructure and the concept of critical information infrastructure. Under critical infrastructure we mainly imply asset, system or some physical part. While critical information infrastructure is "one of the constituent sectors of the overall critical infrastructure, but also is unique in providing an element of interconnection between sectors as well as often also intra-sectoral control mechanism" (Lopez et al., 2012: 1). For the purpose of this view the focus will be placed on the critical infrastructure.

3 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.

The structure of the chapter is divided into four sections: 1. The concept of critical infrastructure protection of individual Member States of the European Union; 2. The normative framework of the European Union in the critical infrastructure protection; 3. Co-operation activities within the European Union; 4. Conclusion. It is started at that way in order to show the solutions of individual states that have begun to develop the area of critical infrastructure protection before the Union and have gradually adjusted. Then we wanted to show the main activities that the European Union undertakes and ways of realization, and to offer a kind of conclusion of this chapter.

2.1. The concept of critical infrastructure protection of individual Member States of the European Union

Before the incentive for critical infrastructure protection came from the European Union level, older Member States of the Union have, in the second half of the 20th century, each for it selves, gradually became aware of the need to protect national critical infrastructures. They have recognized the significance and importance of functioning of critical infrastructure in order to maintain a normal lifestyle of citizens, the functionality of social organization and the functioning of all significant systems in the state. But according to some authors (Setola at al., 2016) focus on protection and resilience of critical infrastructure has come to the fore again in the last two decades.

The importance of exploring this part is multiple and it is reflected in its presentation of: 1. Cross section of the individual endeavours of the analyzed states – their challenges and ways of solving them; 2. Building of normative framework; 3. Review of the reach in this area; 4. Additional challenges faced by states when their policies have to be aligned with EU policies; 5. Guiding idea to other states that are at the beginning of this process. Cross sections of major activities in the United Kingdom, the Kingdom of Sweden and Germany will be presented below.

The United Kingdom belongs to a group of countries that started to develop the area of critical infrastructure protection before the European Union has started to focus on this subject and obligations from the Union level transferred to its legislation by procedural changes in existing critical infrastructure protection activities (Lazari, 2014: 75). The current strategic framework is based on security strategies such as: *The National Security Strategy of the United Kingdom* 2008, 2009, 2010 and 2015, and the *National Counterterrorism Strategy* 2009 and 2011, while the operational framework is contained in the laws regulating key functions in the country, in various interdisciplinary areas such as: protection of information, energy and traffic infrastructure, the functioning of emergency services for extraordinary situations, and other. The United Kingdom in the *National Risk Register of Civil Emergencies* (2008, 2010, 2012, 2013, 2015 and 2017) along with other conditions looks at the risks, threats and weaknesses of the critical infrastructure functioning. That document then serves to all critical infrastructure protection actors as a basis for considering all possible threats and as a platform for planning protection measures.

Critical infrastructure protection lies in the area of policy responsibility of two bodies: the Home Office (Governmental ministerial department responsible

for immigration, security and law and order), which is responsible for protection policies in regards to terrorist threats and the Cabinet Office (Governmental department responsible for supporting the Prime Minister and Cabinet of the United Kingdom), which deals with issues of strengthening resilience and protection from the consequences of natural disasters and catastrophes. Thus, a strategic review and impact on this area has been achieved. The central authority responsible for operational action in order to reduce vulnerability, protect national critical infrastructures, coordinate interdisciplinary activities and actors is the Centre for the Protection of National Infrastructure (CPNI). This Centre is a government authority (established in 2007), which is directly accountable to the Director General of the Security Service MI5 (CPNI, 2017) for its work. The Centre for the Protection of National Infrastructure is an excellent example of established governmental non-profit body that carries out inter-departmental coordination work with companies and organizations from industry, academic community and numerous government departments and agencies. The Centre provides advisory services in order to reduce the vulnerability of national infrastructures from terrorism and other threats. Support to the institutions and to organizations includes also the development and transfer of knowledge about relevant standards and their implementation.

In the UK, nine critical infrastructure sectors and twenty critical services were designated. The ministries responsible for each sector carry out initial selection of assets and operators (operators are selected based on their relative market share). The Centre for the Protection of National Infrastructure conducts its own assessment and selection in parallel. Based on the combined inputs of the operator, competent ministry and CPNI, asset (which can also be a process) is mapped according to the consequences of the potential non-delivery of the service. In the identification process also six levels of criticality are taken into consideration (from CAT0 – "infrastructures whose termination of action would have a minor impact" to CAT5 "infrastructures whose termination of action would have a catastrophic impact on the UK"), which are considered in relation to three specific criteria: impact to life, economic impact and impact on basic (vital) services. Only descriptive and subjective criteria are available to the general public, while at the classified level each criterion has quantitative and objective values (metrics) assigned to them. This segmentation is conducted in combination with sector criteria (specific for each sector) that are unique for each of the nine sectors. Ultimately, a small number of assets were identified according to the highest level of criticality, as only those assets that are in category "CAT3" and above are considered to be really critical. Then, prioritization is being carried out based on "CAT categorization" and probability of attack, which is actually a combination of vulnerability (e.g. ease of access to property) and threats (e.g. type of attack).

The Kingdom of Sweden also started the process of critical infrastructure protection before the initiatives that came from the EU level and has adjusted with amendments to existing laws and bylaws in the area of energy and transport (Lazari, 2014: 75). „From a Swedish perspective, there is no clear definition of what constitutes a critical infrastructure" (Johansson, 2010: 27). Sweden has linked the concept of critical infrastructure with the term of vital societal functions and it

perceives them through a unique concept. Sweden considers critical infrastructure both as critical infrastructure as generally known concept (defined in Directive 2008/114/EC), and as vital societal functions. They are jointly perceived, as opposed to countries like Republic of Croatia which considers critical infrastructure only as physical and vital objects, without including societal functions. In this symbiosis the critical infrastructures present the structures, whose functionalities contribute to the insurance of vital social functions. Those are functions that are so important that their interruption or serious disturbance can pose a great risk or danger to the lives and health of people, the functioning of society or the fundamental social values. This approach to the concept is based on a comprehensive consideration of all risks, threats and weaknesses and the holistic response to them (Swedish Civil Contingencies Agency, 2011). The coordination of the protection of vital societal functions and critical infrastructure is part of the civil emergency preparedness system (Swedish Civil Contingencies Agency 2016), and indicates measures and activities that are being undertaken to ensure the effectiveness and action of critical infrastructures and vital social functions and society as a whole (Swedish Civil Contingencies Agency, 2014).

Central authority responsible for coordinating major activities of the protection of vital societal functions and critical infrastructure is Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap – MSB). MSB is a government authority responsible for issues concerning civil protection, public safety, emergency management and civil defence as long as no other authority has responsibility. Responsibility refers to measures taken before, during and after an emergency or crisis (Swedish Civil Contingencies Agency, 2019). Eleven sectors are identified in Sweden in which is possible to identify and designate vital societal functions and critical infrastructure.

The protection of vital societal functions and critical infrastructure is part of the civil emergency preparedness system, and it indicates the measures and activities that are being undertaken to ensure the efficiency and functioning of infrastructures of importance and vital societal functions, as well as society as a whole. The Swedish Civil Contingencies Agency did initial identification and analyses of the dependence of critical infrastructures based on the authority and guidance of the Government in the period 2006-2008. In that analysis, it was emphasized that vital societal functions are considered instead of infrastructures, because infrastructures were said to only support certain functions of the community. The results of dependency analyses can be used for decisions on prioritizing measures, resource allocation, and focus of studies and research. The Swedish approach to critical infrastructure protection involves cooperation of large numbers of actors, from law enforcement bodies, intelligence and security services, the Swedish Civil Contingencies Agency, sectoral agencies, regional and local authorities to private sector actors who own and operate critical infrastructure.

Germany is example of a country that, like the United Kingdom and Sweden, did the initial alignment of the national legislation in 2001 in the field of energy and in 2002 in the field of transmission systems in order to respond to EU provisions (Lazari, 2014: 74). Although critical infrastructure is protected by numerous regulations, measures and activities, it has decided to specifically arrange this

area. First in 2007, the *Critical Infrastructure Protection Implementation Plan* was launched, which represents a national plan for critical information infrastructure protection. This approach is selected under the premise of the protection of vital national functions through adequate information protection (Federal Ministry of the Interior, 2007). A year later, the *Protection of Critical Infrastructures Baseline Protection Concept* was adopted, which was developed interdisciplinary by public bodies with the aim of providing recommendations to companies on how to strengthen public security through cooperation in critical infrastructure protection (Federal Ministry of the Interior, 2008). Then, in 2009, the *National Strategy for Critical Infrastructure Protection* was adopted, where clearly was highlighted that critical infrastructure protection is a key function of preparedness measures in the area of security activities undertaken by all relevant actors while the mentioned area is central interest of the state's security policy (Federal Ministry of the Interior, 2009). Shortly, in 2011 the *Cyber Security Strategy for Germany* was adopted, which, in addition to other provisions, sees the protection of information infrastructure as the main task of cyber security area (Federal Ministry of Interior, 2011a; 2016), as well as the *National Plan for Information Infrastructure Protection* in which three strategic objectives in critical information infrastructure protection are presented (Federal Ministry of the Interior, 2011b).

At the federal level, the institutional responsibility for coordinating critical infrastructure protection system is at the Federal Ministry of Interior, Building and Community. The Ministry is also a national contact point, responsible for all issues that involve cross-sectoral perspectives and operates the IT Situation Centre and the IT Crisis Centre that follow all important activities related to critical infrastructure. Within the ministry two offices are in charge of some critical infrastructure protection segments – The Federal Office of Civil Protection and Disaster Assistance is responsible for considering comprehensive activities, while the Federal Office for Information Security is focused on cyber protection of critical infrastructures. In addition, for each sector, a competent ministry is designated, responsible for implementing sectoral policies and directing stakeholder activity within the sector. In Germany, nine critical infrastructure sectors were set up in total. At the level of federal states, a system of clear competencies and responsibilities for policy implementation, system management and critical infrastructure protection has also been established.

In Germany there are numerous laws regulating specific sectoral competencies, which relate to the critical infrastructure protection, and also have built-in crisis management provisions (John-Koch, 2017). At the level of legal provisions, two laws need to be set out. First, the *Civil Protection and Humanitarian Aid Act* prescribes provisions on the critical infrastructure protection as a civil protection task (Braubach et al., 2014). Second, *Cyber Security Act*, which approaches to critical infrastructure protection from the position of implementation of minimum standards of information security in the business of all relevant national companies (Deutscher Bundestag, 2015). The *Civil Protection and Humanitarian Aid Act* refers to the functioning of the system as a whole with clearly known competences. While the *Cyber Security Act* specifically applies to more than two thousand companies which provide vital functions/services such as traffic, water management, health

services, telecommunications, maintenance, the financial sector and the insurance industry. A two-year implementation deadline has been set during which time it is necessary to undertake the certification process for new cyber security standards and to renew security certificates. All in order to achieve greater resilience and protection from cyber attacks, and in case of failure to meet the required conditions, the company faces high fines (Ford, 2015; Santillan, 2015). This approach can serve as a model for other countries to regulate area of critical infrastructure protection through more powerful cyber security, because IT systems make the critical infrastructure extremely networked and therefore their protection is of key importance (Kandek, 2015).

These three examples illustrate the diversity of approaches in establishing a normative framework for area of critical infrastructures. From a British example, where only minor changes to the existing laws have been made in order to bring the concept of critical infrastructure into line with the requirements of the European Commission's provisions, which was also the starting action point of Germany, to the case of Sweden where the connection with the concept of vital societal functions formed a unique concept of protection. To date, the United Kingdom and Sweden have maintained a critical infrastructure protection framework through a number of documents at different levels of implementation, while Germany has, after initial alignment, established a completely new regulatory framework for this area. In addition to the mentioned partial differences, all three countries have much more in common. The common denominator for all three states is strong support for the development of public-private partnerships and the necessary cooperation with the private sector in the area of critical infrastructure protection. Then, the identification and designation of critical infrastructures at all three levels of political organization of the country (local, regional, national), which necessitates the daily cooperation between the above levels of government. The emphasis in the implementation of the activity is to assess the risks and vulnerabilities of critical infrastructures and consequently to manage risks and business processes by applying business, industry and sectoral standards. All three countries are striving for the greater cooperation of all involved actors as well as the transparency of the system. Each of the above mentioned models or their combination represents examples to other countries as it is necessary or possible to develop their own national framework for critical infrastructure protection and cooperation of all system stakeholders.

2.2. The normative framework of the European Union in the critical infrastructure protection

The European Union, under the strong impact of the 2001 terrorist attack on the United States, the Global war against terrorism that followed and major terrorist attacks in Europe (2004 in Madrid, 2005 in London), its initial discourse of observation as well as the critical infrastructure protection has set in regard to the defence from terrorism.

In June 2004 the European Council asked the European Commission to prepare an overall strategy in the area of critical infrastructures in the European Union and

to establish a normative framework for its protection. Based on the aforementioned requirement, in October 2004, the European Commission adopted first document in this area entitled *Communication on Critical Infrastructure Protection in the fight against terrorism*, which presented the proposals what Europe should do to prevent terrorist attacks on critical infrastructures, to enhance the level of preparedness for emergency situations, to raise their resilience and to develop the ability to respond to attacks (European Commission, 2004). With this document the intensive work of the European Union bodies has begun, the cooperation with Member States, as well as with individual experts in developing the normative framework and the identity of the Union in the area of critical infrastructures.

One year later, the Commission created a *Green Paper on a European Programme for Critical Infrastructure Protection*, which provided policy options on how the Commission could establish a critical infrastructure protection program and a Critical Infrastructure Warning Information Network (CIWIN) (European Commission, 2005). The discussions that were conducted after the adoption of the *Green Paper* highlighted the added value of setting up the Union's strategic framework for critical infrastructure protection. Also, the key directions of the development of this area are highlighted, such as: the need to improve capabilities for the critical infrastructure protection in Europe and to help alleviate weaknesses related to critical infrastructure. Furthermore, the importance of key principles of subsidiarity, proportionality and complementarity have been highlighted as well as dialogue between stakeholders in the system of strengthening the resilience and critical infrastructure protection (Council of the European Union, 2008).

The next input came from the Justice and Home Affairs Council, which in December 2005 called upon the Commission to make a proposal for a *European Programme for Critical Infrastructure Protection*. The drafting guidelines emphasize that the Programme should take into account all dangers, where priority should be given to countering terrorist threats. Such approach in process of critical infrastructure protection takes into account the technological threats caused by human activity and natural disasters, but priority should be given to the threats from terrorism (Council of the European Union, 2008). Therefore, in 2006, the European Commission adopted a *European Programme for Critical Infrastructure Protection*, which takes all risks into consideration when it comes to critical infrastructure protection, but terrorism remains the primary focus and concern as requested in the guidelines (European Commission, 2006).

In April 2007, the Council of the European Union considered the *European Programme for Critical Infrastructure* and issued conclusions stating that the ultimate responsibility for managing critical infrastructure protection solutions lies on Member States, within their national borders. In addition to this, it is directed to the Commission to develop a European procedure for identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Mentioned is an important determinant of the development of this area, as it is recognized that there are a number of critical infrastructures in the Union which disruption of work or destruction could have significant cross-border effects. Work disruptions may include cross-border cross-sectoral effects resulting from the interdependence of mutually connected infrastructures. Bilateral

cooperation programs between Member States in the area of critical infrastructure protection represent a well-established and efficient tool for dealing with cross-border critical infrastructures, but the need for integrated solutions at the level of whole Union is recognized. Therefore, it was necessary to set the conditions for the identification and designation of the European critical infrastructure through the joint process of Member States, their mutual cooperation and the inclusion of the owner or operator in the above mentioned processes (Council of the European Union, 2008).

In parallel with the work of the Commission, the Council of the European Union adopted in 2007 a special program the *Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*. This program identifies a number of security-related risks, with the focus on supporting Member States' efforts to prevent terrorist attacks and to carry out preparations for the protection of people and critical infrastructure from risks related to terrorist attacks (Council of the European Union, 2007).

After that, the Council of the European Union, taking into account the proposal of the Commission, has brought immediately a key document for the area of critical infrastructures in the European Union, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (further *Directive 2008/114/EC*), which is no longer primarily focused on the threat of terrorism, but seeks to establish a comprehensive process of critical infrastructure protection both at the level of the Member States and the Union as a whole (Council of the European Union, 2008). Legal basis of the *Directive 2008/114/EC* is Article 308 – *Treaty establishing the European Community*. It is noticeable, the Union's initial discourse on critical infrastructure protection was primarily directed at the defence of terrorism. Over time, other risks are increasingly respected and discussed, but terrorism remains the declared major threat. Until the adoption of *Directive 2008/114/EC* when a comprehensive approach of consideration of all risks and threats was presented.

Although the mentioned documents of the European Union, as well as many others brought by the Union, have suggested the definition of critical infrastructures, by adopting *Directive 2008/114/EC* the definitions set out therein have become a sort of theoretical constraint for national critical infrastructures and European critical infrastructure from Union institutions to Member States. States have started to use in their documents identical definitions or very similar modifications. According to *Directive 2008/114/EC*, critical infrastructure means "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." European critical infrastructure means "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure" (Council of the European Union, 2008). *Directive 2008/114/EC* applies from 12 January 2009, while the Member States should have

included it in the national legislation until 12 January 2011, in the sectors of energy and transport, and the candidate countries for full membership in the European Union must implement *Directive 2008/114/EC* before joining the Union.

The suggestion that members of the European Union, following the adoption of *Directive 2008/114/EC*, are obliged to incorporate its provisions into national legislation has become a multiple challenge because the "older" EU Member States have begun the process of critical infrastructure protection prior to the adoption of *Directive 2008/114/EC* so this is potentially an obstacle in the implementation of their own policies, but they are required to harmonize national policy with the Union's policy in this area. The new Member States found themselves in the need for quick adaptation or opening up the process for the first time although some of them were not yet fully organizationally ready for that purpose. But *Directive 2008/114/EC* left no room for them to be postponed and did accelerate their adjustment. The question that arises is how much this presented a problem and a challenge to them, and how much did that accelerate their preparations and directed them to solving the matter directly. Advantage for new Member States of the Union, if they have not developed policies, measures and activities in the critical infrastructure protection until the adoption of *Directive 2008/114/EC*, is that they are not burdened by previous approaches, and on the basis of EU regulations they have the ability to develop and implement new ideas that may be of benefit to the Union as a whole and to older members in the policy of critical infrastructure protection.

As critical infrastructures are connected and increasingly dependent on the Internet and processes in the cyberspace, the Union has had to take steps to regulate this area. In 2013, the European Commission, together with the High Representative of the European Union for Foreign Affairs and Security Policy, put forward a *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* which represented the EU's comprehensive vision on how to best support Member States and other stakeholders in preventing and responding to cyber disruptions and attacks (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013). "The vision was to foster European values of freedom and democracy and to ensure that the digital economy can safely grow. Specific actions aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber security and cyber defence policy." The Strategy articulates the EU's vision of cyber security through five priorities: 1. Achieving Cyber Resilience; 2. Drastically reducing cybercrime; 3. Developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); 4. Developing the industrial and technological resources for cyber security; and 5. Establishing a coherent international cyberspace policy for the European Union and promote core EU values. Strategy is implemented via a series of instruments: Legislative instruments; Non-legislative instruments; and Funding activities (European Commission, 2017: 2-3). The Strategy is an essential basis for further joint activities in the regulation of cyberspace as well as the critical infrastructure protection in that dimension because "securing network and information systems in the European Union is essential to keep the online economy running and to ensure prosperity" (European Commission, 2019).

Based on a *Cybersecurity Strategy of the European Union*, 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* (further *NIS Directive*) was adopted. It was adopted on 6 July 2016 with the obligation to be implemented into national legislation of all Member States until 9 May 2018 (European Parliament and of the Council, 2016). The *NIS Directive* presents main piece of legislation of the *Cybersecurity Strategy of the European Union* and is extremely significant in its nature and application. Legal basis of the *NIS Directive* is in Article 114 – *Treaty on the Functioning of the European Union*.

2.2.1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Since *Directive 2008/114/EC* represents the central point of EU policy development and the Member States, accession countries and candidate countries for EU membership, it sets the logic of establishing business processes and the basis for a number of other activities (such as EU funded projects, development of cooperation between states and critical infrastructure operators, establishment of public-private partnerships, development of curriculum, foundation of centres and summer schools with special interest in critical infrastructures ...), it is necessary to pay a special attention to its analysis, its significance, the reach, and the challenges of its application.

In the introductory provisions of D*irective 2008/114/EC*, the Council of the European Union has taken steps to highlight the essential guidelines for all those concerned. It was emphasized that the first step in the multiphase approach is aimed at identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Then, that focus is primarily on the energy and transport sectors, but other significant sectors such as information and communication technology sectors need to be considered. As well, and what is especially important, that the Member States and the owners or operators of the above mentioned have the primary and ultimate responsibility for the critical infrastructure protection in Europe. This was an extension of the protection obligation issued by the Council in April 2007 when considered the *European Programme for Critical Infrastructure Protection* and adopted conclusions on the protection of national critical infrastructures emphasizing that the ultimate responsibility for protection is on Member States. Because ultimately European critical infrastructures are primarily national, and when they are of mutual significance for two Member States, they are identified as European.

The next important aspect of *Directive 2008/114/EC* is that it has become a common platform for the cooperation of all relevant stakeholders of the critical infrastructure protection system at Union level. Prior to its adoption, the obligation of official cooperation among various stakeholders, as well as the forum for achieving this cooperation, did not exist. Its strenght is in mandatory application, and each Member State chooses the way how it will be transposed into national legislation. States have previously cooperated bilaterally but could not fully achieve a higher

level of operationality in developing a process for identification and designation of common (European) critical infrastructures as well as a common approach for the assessment of the need to improve the protection of such infrastructures, so there was a necessity for coordinate action coming from the Union level for which the *Directive 2008/114/EC* set the base.

The central part of *Directive 2008/114/EC* is the procedure for identification and designation of European critical infrastructures. The identification procedure was adopted in Article 3 and the accompanying attachment. It consists of several steps involving the terminology equivalence of the observed infrastructure according to the set definition and the fulfilment of the cross-cutting and sectoral criteria. The first step is that each Member State applies sectoral criteria to make the primary identification of critical infrastructure within the sector on the national territory. Sectoral criteria are the first selection of potential critical infrastructures. The second step is to apply definitions to the considered infrastructure in order to see if it meets the "critical infrastructure" requirements/conditions as well as "European critical infrastructure". The third step is to look at the cross-border impact of the definition of "European critical infrastructure" and to determine whether a certain infrastructure is mutually significant for two Member States, whether the both determined it as a significant or that one of the member finds that there is infrastructure on the territory of the other Member State that is significant to her alone. The fourth step is the application of cross-cutting criteria that include the observation of three criteria:

a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);
b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services) (Council of the European Union, 2008).

If needed, the European Commission can assist Member States in identifying potential critical European infrastructures for any reason – lack of administrative and professional capacity, lack of procedures or uncertainty in the interpretation of certain criteria, lack of co-operation with another Member State, up to inactivity where the Commission can draw attention to some Member States to the existence of potential critical infrastructures that can be considered to fulfil conditions, to be identified first and then designated as critical European infrastructures.

The procedure for designation of critical European infrastructures was adopted in Article 4 and can be done after the procedure for identification of potential European critical infrastructures has been carried out. If a Member State has identified potential critical infrastructures on the territory of other Member States or has found that there is infrastructure on its territory that is significant to neighbouring countries – it will inform them of this. Only infrastructure which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people comes into consideration and the

disruption or destruction of which would have a significant impact on one or both of the Member States. It then follows the process of bilateral and/or multilateral discussions between the States in order to look at the situation and the potential adverse effects of the downtime and/or the breakdown in work of the established infrastructure. At the invitation of the Member States, the European Commission may participate in these discussions. After the analysis has been carried out, in order to identify the potential critical infrastructure as a European critical infrastructure, the consent of the Member State on whose territory mentioned is located and is designated as a critical European infrastructure is required. In the case of impossibility of reaching agreement between the Member States, they can address to the Commission, which may be involved in the discussion and facilitate the achievement of the agreement between the States (Council of the European Union, 2008).

Following the successful negotiations between the Member States, the next step is to inform the owner or operator of the critical infrastructure that his infrastructure has been identified and designated as a European critical infrastructure. The Member State on whose territory this European critical infrastructure is located is responsible for informing the owner or operator, and is also obliged on annual basis to inform the Commission of the number of designated European critical infrastructures per sector and of the number of Member States dependent on each designated European critical infrastructure. The information on the designated infrastructure is classified according to the appropriate level of data secrecy and their identity is known only between the Member States that shares mentioned infrastructure and/or are in any way dependent on it. The Commission's interest is to receive from the Member States as comprehensive information as possible on risks, threats and weaknesses in the sectors where European critical infrastructures are designated, as well as information on cross sector dependencies and steps taken to reduce risks, threats and weaknesses in order to develop appropriate proposals aimed at protection of observed infrastructures.

After that, in designated European critical infrastructures, it is necessary to set up operator security plans of critical infrastructures or equivalent documents which include the identification of important assets, risk assessment and selection and prioritization of countermeasures and procedures for the protection of those assets. In order to avoid unnecessary work and duplication of documents, each Member State should first determine whether owners or operators of the designated European critical infrastructure have already established operator security plans or other equivalent documents. Where such plans exist, it is necessary to analyze them and see if they need to be upgraded, and where they do not exist, each Member State should take the necessary measures to ensure the establishment of the mentioned.

The next important provision is to determine Security Liaison Officer. The state needs to ensure that each owner or operator has appointed a security coordinator within the European critical infrastructure or the security officer in charge of security affairs. The mentioned is an important horizontal and vertical link between the elements of the critical infrastructure system as well as the contact person with the legislator and other critical infrastructures. And the state needs to appoint a

national contact point in charge of co-operation with the Commission, other states as well as with the owners or operators of the European critical infrastructures designated on its national territory.

Directive 2008/114/EC has set a number of practical solutions that, in addition to the regulatory obligations of the area of European critical infrastructure protection, serve the states for designing internal processes related to the national critical infrastructures protection. An example of this is the establishment of the legislative framework of the Republic of Croatia where the legislator largely decided to fully follow the narration and content of *Directive 2008/114/EC* in the development of the *Critical Infrastructure Act*.

Following the adoption of *Directive 2008/114/EC*, Member States have faced the challenge of adapting the national frameworks or for the first time establishing a whole set of program related to the critical infrastructure protection. Some consulted sources (Lazari and Simoncini, Haemmerli and Renda) consider that following the adoption of *Directive 2008/114/EC*, the following steps required by the Commission in the development of the area were absent and there was a vacuum in which Member States were more or less left to themselves. Although, *Directive 2008/114/EC* provides clear provisions, monitoring of its implementation in national legislation has been left out. Alessandro Lazari and Marta Simoncini point out that *Directive 2008/114/EC* is incorporated into each of the 28 national laws of the Union's Member States, namely: "amendments to existing laws and subordinate legislation (4 states); new laws (9 states); resolutions (4 states); procedural changes in existing critical infrastructure protection activities (3 states); decrees and execution provisions (8 states)", but not all countries have transposed the spirit of *Directive 2008/114/EC* in the required way (Lazari and Simoncini, 2014: 13). The Commission, after adopting *Directive 2008/114/EC*, did not have a clear goal of how to guide and model the process. There was a lack of a cohesive factor by which the Commission would allow Member States to adopt the standards as best as possible and in required spirit implement the provisions of *Directive 2008/114/EC* (Haemmerli and Renda, 2010). The same authors (2010: 7) further consider that in years after the adoption of *Directive 2008/114/EC* "EU Member States are still pursuing fragmented C(I)IP policies, and there is still a significant lack of cooperation between national governments and EU institutions in setting up a coordinated emergency response to potential threats."

Directive 2008/114/EC should be observed in the scope and time when it was adopted. Certainly it was a huge step forward, but clearly, it could not respond to all requirements of complete regulation of the area for identification, designation, and protection of European critical infrastructures. At the same time, it had to partially level the already developed national policies of individual Union's Member States with those who did not pay enough attention to this area or started just now, under its impact, to regulate this area. *Directive 2008/114/EC* was originally used to guide Member States in their mutual cooperation and as an example of how they can directly establish and organize the national framework for identification and designation of critical infrastructures and indirectly for their protection. It was further on Member States to develop this area with the help of the Commission and not for it to have a main role. Illustrative of the above may

be a brief analysis of three countries: Italy, Romania and Croatia – and how they have responded in the early years following the adoption of *Directive 2008/114/EC*. Italy has not recognized the spirit of *Directive 2008/114/EC* nor has it taken advantage of the possibility of enhancing transparency, the effectiveness of cooperation in the critical infrastructure protection and has not clearly defined the obligations and responsibilities of the owners or critical infrastructure operators in the national context. Romania has co-opted the spirit of *Directive 2008/114/EC* and has regulated its legislation in accordance with the provisions of *Directive 2008/114/EC*. It has organised processes, built a system of critical infrastructure protection, established functional forms of support to public institutions and owners or critical infrastructure operators in their tasks, and this works in practice (Lazari and Simoncini, 2014). Croatia has established a normative framework in accordance with *Directive 2008/114/EC*, set up system architecture and selected Security Liaison Officers in the competent central state administration bodies, and for years has invested in efforts to designate national critical infrastructures, educate Security Liaison Officers, held meetings with Slovenia and Hungary on establishing European critical infrastructure, carried out the EU funded project RECIPE 2015 with an aim for further developing of started activities of system building. However, since nothing in these efforts has given concrete results, after several years a complete "deadening" of the process has taken place. In order to avoid being misunderstood, this comment refers to the activities of the mentioned three countries since the adoption of *Directive 2008/114/EC*, through its obligation of implementation in national legislation and looking at the efforts made in several years, till 2014 in the case of Italy and Romania, and 2015 for Croatia. After this period, all three states had specific concrete activities and results, where Romania is the predominant one.

2.2.2. 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

Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities and in particular to the functioning of the internal market. The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union (European Parliament and of the Council, 2016: 2). That is why the *NIS Directive* was adopted to connect the key areas, actors and processes, in order to increase the level of protection and the introduction of minimum common standards in this area.

The *NIS Directive* covers two groups of actors: Operators of Essential Services and Digital Service Providers. Under the Operators of Essential Services are considered those who provide key services to society or the national economy in the following seven sectors: Energy, Transport, Banking, Financial Market, Health,

Drinking Water Supply and Distribution, Digital Infrastructure. Digital Service Providers are considered to be of general importance when it comes to cyber security and include providers in the following three sectors: Marketplaces, Cloud Computing Services and Online Search Engines.

The main objective of the *NIS Directive* is to provide a common level of security of network and information systems in all Member States, whose malfunctions due to security incidents may have strong consequences on society or the national economy. In doing so, the *NIS Directive* introduces regulatory elements that enable permanent monitoring of the condition of automation and digitization of the designated sectors. In addition, it introduces the obligation to implement technical and organizational measures for risk management and measures to prevent and minimize the effect of the incident on the security of network and information systems, and introduces an obligation to notify about incidents that may have a significant effect on the continuity of service providing.

Observing the *NIS Directive* in relation to *Directive 2008/114/EC*, it is necessary to highlight several important issues. We can say that the *NIS Directive* has been developed from the need to complement the normative framework, because of the lack of adequate critical infrastructure protection and operations in the information and communication technology sectors. *Directive 2008/114/EC* focuses primarily on energy and transport sectors but also emphasize the need that other significant sectors, such as information and communication technology sectors, to be considered. Then, Operators of critical infrastructures and Operators of Essential Services do not necessarily coincide, but there is also a great likelihood that they will overlap in many cases. *Directive 2008/114/EC* is more focused on assets, while the *NIS Directive* is more focused on services. The main objective of the *Directive 2008/114/EC* is restricted to enhancing the security of specific critical infrastructures that are important at EU level, while on the other hand *NIS Directive* main objective is enhance the overall EU network and information security via Member States security and EU cooperation.

2.3. Co-operation activities within the European Union

The Centre for European Policy Studies Task Force on Critical Infrastructure Protection considers that, although the Commission has adopted numerous policy initiatives in this area, a number of outstanding problems remains. "First, Member States are at varying degrees of maturity with respect to the development of a comprehensive and effective CIP policy. Second, there are islands of cooperation across the EU Member States but no overall concept of operations at the EU level. Third, partnerships and relationships are scattered across countries (each individual country has and will maintain unique relationships with private sector owner operators and global companies that enable them). Fourth, critical EU infrastructure is also scattered across many different countries" (Haemmerli and Renda, 2010: 3). It should be noted that some of the mentioned challenges have been solved, but some are still present.

Certainly there are challenges, as they are present in every business environment and process. They are an integral part of business, cooperation, exchange of

knowledge, establishment of new systems and improvement of existing ones. The dynamic world we live in is such that it expects rapid progress in all areas and activities we are dealing with. But the reality of mosaic alignment that we call the European critical infrastructures – and which is woven out of a multitude different actors with multiple roles, physical and virtual structures, large amounts of IT solutions (which are outdated before most have been able to figure out how they work), frightening quantities of information which need to be stored, protected and analyzed, different levels of regulation, countless spheres of impact and interest – for which we can safely say is a "living organism" that constantly changes, grows and draw in new amounts of information, technology, sensors, finance all the way to people – we cannot put in a "frame" and expect quick solutions. Here we can apply two different approaches towards the totality of functioning. The first approach is with reductionistic point of view, according to which, such an organism is simply not subject to quantification or management of the entire volume, but access to it should be based on the analysis of individual parts, their overall contribution and management of mentioned. The other approach is from a holistic aspect, which perceives the whole organism, with all its parts and respecting cross-sector understanding.

According to this, no single institution of the Union can simply be apostrophised that it has not invested more effort in the development of the area of critical infrastructure protection. At the end, everything is the result of the work of people involved on tasks of critical infrastructures and their productivity. We have witnessed various activities implemented at Union level or within a national framework where the contribution of those involved was insufficient to achieve the foreseen goals, this way leaving no result and progress. All of this is an integral part of life and perspective of life priorities. Thus, it is necessary in the analysis of the so far achievements of the development of area of critical infrastructure protection to look at the anthropological, cultural, organizational and other factors of an individual environment, individual organizations, states, sectors and to see why some environments are more successful than others. It is not our aim to defend the EU institutions but to show their main activities in this area, which then testifies to the many missed opportunities by the users whether they are the states, owners or operators of critical infrastructures, regulatory agencies, the scientific community, or individuals. The Union develops this area with great transparency, everyone has the opportunity to get information and be part of the activity, but the question is whether they have decided on it.

In order to support Member States, the Commission has also engaged its own Joint Research Centre, which in 2008 produced a document entitled *Non-Binding Guidelines for application of the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection*. The document aims to assist Member States in the proper application of technical provisions for the determination of European critical infrastructures (Lazari, 2014: 52). It is aimed at what is most challenging to all Member States when they first open the process of identification and designation of critical infrastructures – and this is a detailed explanation of the correct application of sectoral and cross-cutting criteria. It is proposed to use four different criteria/ conditions for cumulative observation of the sectoral criteria:

1. Prescribe specific properties (according to its necessity for the functioning of the entire system, sector and/or organization);
2. Identify networks of which the 'key elements' must be determined (according to the potential negative effects that may occur in the Member States);
3. Name a specific infrastructure asset directly;
4. Allow an Member States to identify an asset directly (in the cases where no sectoral criteria exist) (The Joint Research Centre, 2008: 23-24).

The above criteria/conditions represent as the title of document says – non-binding guidelines that should make it easier for Member States to open proceedings for the first time. If states have developed better-quality criteria, they should definitely use them, and the document suggests ideas from which way to go. In the interpretation of cross-cutting criteria (criteria are: a) Casualties criterion; b) Economic effects criterion; c) Public effects criterion) a detailed description of the qualification and quantification of the above criteria is provided and a very important interpretation is given that it is sufficient that one of the three criteria is satisfied in order to fulfil the condition for the application of cross-cutting criteria (a fourth step is considered to be met in the procedure of determining European critical infrastructure) (The Joint Research Centre, 2008: 25-35).

After that, the Commission has put its focus on the development of various platforms for cooperation between Member States, owners or operators of critical infrastructures and interested experts. A concrete measure is to hold meetings for national contact points within the official format of the European Commission, which is usually organized twice a year. At these meetings Member States have the opportunity to exchange best practices and achievements at all phases of the protection of national and European critical infrastructure. In this process, the Commission is the organizer and moderator, pays the costs of participation of all national contact points, prepares meeting materials, presents the latest relevant results of various programs and projects, supports initiatives and most importantly – allows Member States to co-operate. How successful this co-operation is and everything that is enabled to Member States depends on numerous factors on which the Commission has no direct impact, and some of the following are: what importance is given to that process referred within the national framework, how national contact points understand and accept the process, the quality of cooperation between the security coordinators within the national framework and similar.

In addition to this formal network, the Commission strongly encourages Member States to participate with their representatives in the informal network of experts within the framework of the European Reference Network for Critical Infrastructure Protection (ERNCIP). The network aims to provide a framework within which experimental facilities and laboratories share knowledge and expertise in order to align test protocols across Europe, which leads to better critical infrastructure protection from all kinds of threats and dangers and creating a single market for security solutions. At present, within the mentioned, the work takes place in twelve working groups, all of whom have a duty to constantly examine and improve the numerous standards and procedures in the critical infrastructure protection (The Joint Research Centre, 2017). The network presents a true scientific excellence

mine that publishes a lot of significant studies, organizes educations, develops new programs and provides support to all interested. Although it represents a good source of knowledge and potential co-operation, it is surprising that only slightly more than half of the Member States actively participate through their representatives at working meetings, and only a small part of it actively cooperate. This can be linked to the previous statement related with cooperation factors to which the Commission has no direct impact, and also this is additionally influenced by the individual understanding of the importance of investing in knowledge and research. Considering this, we can very easily associate that states, that otherwise invest in research and development, are also active in this section, while others are passive observers.

The next significant opportunity, that the European Commission provides to all interested actors in the area of critical infrastructure protection are projects. Through the program the *Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*, during the period 2007-2012, 111 projects were co-financed (70 – directly related to critical infrastructure protection, 32 – related to crisis management, 9 – mixed) with a total of 45 million Euros allocated. The projects had a very wide coverage and included all sectors in which critical infrastructure could be identified. The main purpose of this programme was: to ensure the improvement of knowledge, a better understanding of the functioning of critical infrastructure at all levels, to provide recommendations to public policies and assure scientific groundwork to current and future research. Some areas that were involved include: analysis of sectoral and cross-cutting criteria and benchmarks; defining various methodologies for assessing interdependencies between critical infrastructures; drawing up best practice guides for public policy makers in critical infrastructure protection; models for exchange of best practices for effective critical infrastructure protection; modes of data exchange and warning systems; development of simulation models and tools for cross-cutting criteria (European Commission, 2013: 6). After this period, the Commission continued to invest in projects that enable to all interested co-financing the projects costs to the greatest extent and most importantly the transfer of the required knowledge and technology. More recent data show that a total of 140 million Euros have been invested in operational cooperation and activities in the period 2007-2013 and more than 120 projects have been financed up to now (Engdahl, 2016: 4). Again, as in the previous cases, how much someone uses the above mentioned options depends only on the end user. The Commission supports every good idea.

The next important step in establishing cooperation and exchange of knowledge and experience at the European level was designing and launching of Critical Infrastructure Warning Information Network (CIWIN). This was already announced in the *Green Paper on a European Programme for Critical Infrastructure Protection* in 2005, and has been gradually created by a modular approach and has become operational in January 2013. The purpose of the network is to exchange information on strategies and measures to reduce risk in critical infrastructure protection. It has been developed as a protected web platform of European Commission for all interested experts of EU Member States dealing with area of critical infrastructure. Approval for access to the network is very simple,

and it provides numerous opportunities such as reviewing normative solutions, studies, best practices, and contacts with other experts. As in previous cases, the Commission has provided a platform for cooperation and those who are interested can use above mentioned options.

This is just a part of the Commission's activities on creating the assumptions and linking different stakeholders of the critical infrastructure protection system. There are still enough of these activities, but we consider that we have touched those more important and have sufficiently presented the Commission's work in this area.

Also, the Commission has recognized the standstill in the normative area of the developing process of the area for identification and designation of European critical infrastructures as well as in cooperation between Member States, and in 2012 it has started to carry out a revision of the previous activities and the development of a working document dedicated to a new approach in critical infrastructure protection. In mid-2013, it presented the *Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure*. The above is an updated version of the European Programme, originally adopted in 2006. The solutions proposed so far have been reviewed, a new look at ways and models on how to continue to develop this area is presented, including some data such as: how less than 20 European critical infrastructures are designated, and among them aren't for example the main energy distribution network (European Commission, 2013). By 2016, in total 89 European critical infrastructures (Engdahl, 2016: 3) were designated. The latest data from the beginning of 2019 is that 92 European critical infrastructures are currently designated.

The Working Document presents a new look at the more practical implementation of the *European Programme for Critical Infrastructure Protection*, provides an analysis of the elements of the current program and proposes a transformation of the approach of European critical infrastructure protection, based on the practical implementation of activities within the area of prevention, readiness and response. Part of the new approach is to look at the interdependence between critical infrastructure, industry and state entities, as it has been noted that the interdependence so far has not been sufficiently percieved. As many of the critical infrastructures are in private ownership, it confirmed the view that better co-operation with the private sector and the development of public-private structured dialogue are needed.

Four priority areas of the European critical infrastructure protection model are additionally highlighted, which need to be further elaborated: 1. Procedures for identification and designation of European critical infrastructures and the assessment of the need to improve their protection; 2. Measures designed to assist the implementation of the *European Programme for Critical Infrastructure Protection*, including the Action Plan, the establishment of a Critical Infrastructure Warning Information Network (CIWIN), the use of expert groups for critical infrastructure protection at Union level, exchange of information, identification and interdependency analysis; 3. Financing of measures related to the critical infrastructure protection and projects associated with a special program *Prevention,*

Preparedness and Consequence Management of Terrorism and other Security-related Risks; 4. The development of the external dimension of the *European Programme for Critical Infrastructure Protection* (European Commission, 2013).

With a new approach, the Commission seeks to improve the critical infrastructure protection throughout the Union, to set up the entire process to a higher level and to create a platform for sharing information and best practice by setting up expert groups for each sector. A pilot project was set up in the new approach, the *European Programme for Critical Infrastructure Protection*, which for the consideration of the interdependence between the various critical infrastructures significant for Europe, determines the following: Eurocontrol, Galileo, electricity transmission network and gas distribution network. These systems are selected because of their relevance to the European Union and in order to optimize their protection and resilience (European Commission, 2013). The aim of the project is to show that the European Commission will independently carry out interdependency analysis of these systems, which should help Member States in their work. The project has been delayed several times since the beginning and has not yet been completed.

At present, the key activity carried out over the last few years, at the Commission's initiative, is the revision of *Directive 2008/114/EC*. So far, its evaluation has been carried out by the Commission to check: its effectiveness in achieving the goals (identification and designation of European critical infrastructures and the assessment of the need to improve their protection); whether it is relevant in consideration of current and future challenges for critical infrastructures and whether it is coherent and complementary with regard to EU and national policies in the focal areas (energy and transport sectors), or which is its added value in that sense. Evaluation also gives recommendations on how to improve operationalization at national levels while maintaining strategic focus; monitoring; synergy on the national level (sectoral legislation); exchange of information and cooperation with third countries, and etc. During several months of evaluation preparation, a workshop was held in Brussels in November 2018 – of Member States together with operators/owners of critical infrastructures, where on a case study a simulation of the process for identification and designation of European critical infrastructures was conducted in accordance with *Directive 2008/114/EC*. A number of implementation questionnaires have been conducted (identified and designated European critical infrastructures, risks, threats and vulnerabilities of the European critical infrastructure sectors) in order to obtain as much information as possible from all stakeholders crucial for the implementation of *Directive 2008/114/EC*. As a final product, the evaluation has brought identified challenges in implementation, the best practices of individual Member States, conclusions and recommendations what is presented in the final, very comprehensive document (90 pages with 500 pages of attachments). Based on this evaluation it will be determined in the next step what will happen with *Directive 2008/114/EC*. Will it change or create a whole new document (about which format will be afterwards decided) that will completely replace it (Cesarec, 2019).

Chapter conclusion

The critical infrastructure protection in the European Union is a complex and dynamic process that takes place on a daily basis at a multitude of different levels and perspectives. In it the main actors and initiators are the states and individual institutions of the European Union, although some owners or operators of critical infrastructures have knowledge and abilities that go beyond the above mentioned. This is logical because they represent the essence of the system and know best their own specifics, risks, sectoral logic and perspective. In addition to the above, experts in the area of critical infrastructure protection are increasingly profiling, bringing added value to the system through their interdisciplinary knowledge and skills.

This chapter was intended to present the historical cross-section of the individual activities of selected states that started, before the input from the EU level came, to deal with the issue of protecting their own critical infrastructure. What was then needed to be aligned with the efforts of the EU institutions to standardize the common area, assist Member States in their challenges, introduce consideration of a place and the role of European critical infrastructures, and to clearly realize their own visibility and recognition in this area.

The main normative solutions and suggestions of the Union institutions in this area are presented and analyzed. The Union has done a lot in the development of this area, and reasons why certain processes have not been faster and/or more efficient we can attribute to the human factor primarily in the Member States rather than in the Union institutions. The Union has worked as strong as the Member States have required and have looked for new and better solutions. Without wanting to be critical, a lot has been done, there are missed opportunities, but this is a dynamic and extremely interactive area that will get more and more space and time in all spheres of political, social and security activity, because every day we depend more and more on the effective functioning of critical infrastructures.

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