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 11
Introduction 13

1. Critical Infrastructure: Notion and Concept
1.1. Defining Critical Infrastructure 19
1.2. Threats and risks to Critical Infrastructure 22
1.3. The need for Critical Infrastructure Protection 28
1.4. Indicative list of Critical Infrastructure 36
1.5. Standard for Critical Infrastructure Protection 39
Chapter conclusion 43

2. Critical Infrastructure Protection in the European Union
2.1. The concept of critical infrastructure protection of individual Member States of the European Union 48
2.2. The normative framework of the European Union in the critical infrastructure protection 52
2.3. Co-operation activities within the European Union 61
Chapter conclusion 67

3. Critical Infrastructure Protection in NATO
3.1. Strategic Framework of Critical Infrastructure Protection Concept 72
3.2. Involvement and Role of the Alliance in Critical Energy Infrastructure Protection 74
3.3. Critical Review of the Complex Role of the Alliance 82
Chapter conclusion 87

4. Critical Infrastructure Protection in the United States
4.1. The Organizational Structure of Critical Infrastructure in the United States 91
4.2. Public-Private Partnerships: The Roles and Responsibilities of Critical Stakeholders 96
4.3. National standards and the Role of the Government in Policy and Enforcement 102

4.4. Critical Infrastructure Sector Interdependency 106
4.5. Future Landscape of Critical Infrastructure in the United States 109
Chapter conclusion 110

5. Critical Infrastructure Protection in Croatia

5.1. The period until the entry into the European Union 116
5.2. Establishment of a regulatory and strategic framework for critical infrastructure protection 118
5.3. Structural Challenges in Establishing a Critical Infrastructure Protection System 130
Chapter conclusion 136

6. Republic of North Macedonia and Critical Infrastructure Protection

6.1. Conditions in the Republic of North Macedonia in the Field of Critical Infrastructure Protection 141
6.2. Protection and Security of Critical Infrastructure in the Republic of North Macedonia 143
6.3. An Example of Creating an Effective Strategy for Critical Energy Infrastructure Protection 144
6.4. Legal Norms and Shortcomings for Adoption of Energy Infrastructure Protection Strategy of the Republic of North Macedonia 146
6.5. Elements and Model of a Strategy for Energy Infrastructure Protection 152
Conclusions and Recommendations 155

Literature 159
Index 170
About authors 173

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 1

CRITICAL INFRASTRUCTURE: NOTION AND CONCEPT

CHAPTER 1

Critical Infrastructure: Notion and Concept

Marina Mitrevska, PhD
University of Ss Cyril and Methodius - Skopje
Faculty of Philosophy, Institute of Security, Defense and Peace

1.1. Defining Critical Infrastructure

The term "critical infrastructure" is relatively new and theorists find its roots in the mid-nineties and it is closely related to energy security, telecommunications, energy systems, gas and oil pipelines, the economy, transportation, water supply and so on (DCSINT 2006: 1). For these reasons, "critical infrastructure" and its effectiveness are of great importance for the quality of life, economy and functioning of the public sector. Today's turbulent world and dynamic development with the increasing penetration of modern technologies and artificial intelligence, the increased number of non-specific threats and risks, as well as the ever-increasing effect of climate change resulting in more frequent disasters and increased intensity and huge damages and losses, affect the notion of "critical infrastructure" to be ever more prevalent in everyday life.

From a research perspective, the interest for the meaning of the term "critical infrastructure" can also be seen through a simplified approach. Namely, if the term "critical infrastructure" is searched via scholars google.com, it is obvious that at the moment 298.000 research results are identified, which represents a huge database of papers related to the term "critical infrastructure" (accessed on April 1, 2019).

Subsequently, the terminological and theoretical frameworks of defining "critical infrastructure" in literature have been built. Understanding "critical infrastructure" moves within the framework of describing critical infrastructure as an important component of the national security of each state, since endangering such facilities/infrastructures brings into question the normal course of life and safety of citizens, as well as the general functioning of the state (Mikac, Cesarec, Larkin, 2018: 23) or as a set of all objects, systems, networks and functions, vital for the survival of the state, whose destruction will negatively affect safety, national security, public health, etc. (Dawson, Omar, 2015: 97).

According to Moteff and Parfomak, critical infrastructure is the basic facilities, services, and installations needed for the functioning of a community or society (Moteff and Parfomak, 2004: 5). On the other hand, in the process of overall contemporary development and the dominant automation and digitalization of all segments in societies, critical infrastructure is a complex system that is specifically exposed and vulnerable primarily to natural threats, technical and technological hazards and antagonistic threats. In this context, Mottef and Parfomak believe that the term "critical infrastructure" should be broadened from what is primarily

for national defense, economic security to what is of vital importance for public health, security and national morality.

If these systems are at risk, that is, deficient or destroyed, there will be an impact on the economy, psychology and security of the nation and society (Levis, 2006: 1). This can be seen in numerous definitions of "critical infrastructure" in literature, and its protection and the need to strengthen the resilience of society becomes a challenge and an attractive subject for research. However, most often, everything comes down to the fact that the infrastructure, systems and resources are of vital importance for a society. High interdependency of these systems with other systems of social life requires more attention to be paid to their protection (Keković, 2013: 203). Perhaps that is why different countries define critical infrastructure in a different way. Let us take a look at some of them.

The United States began to develop this area in the middle of 1990s, and in 1998 in the Presidential Decision Directive NSC-63 defined critical infrastructure as "physical and cyber-based systems essential to the minimum operations of the economy and government". Immediately after the terrorist attack on New York and Washington on September 11, 2001, the Congress passed the Patriot Act in which critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national, economic and social security, the stability of economy, etc" (Patriot Act, 2001). In addition to this, the argument is that with the adoption of the Patriot Act, the United States' activities for critical infrastructure protection are closely linked to defense and terrorism.

Australia is a country that, together with the United States, has begun the theoretical development of critical infrastructure area. Australia defined critical infrastructure as, "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defense and ensure national security" (National Guidelines for Protection Critical Infrastructure from Terrorism, 2011: 3).

In the United Kingdom, critical national infrastructure includes assets, services and systems that support social, economic and political life and their destruction can cause casualties, have impact on national economy, social consequences or be a priority goal of the Government.

In Germany, the term "critical infrastructure" means the organizational structure and facilities of vital importance to society, so that their degradation and deficit would result in deficiencies, cause substantial decrease in supply, disruption of public order and other consequences".

National critical infrastructure of Croatia encompasses "systems, networks and facilities of national importance, where their termination of work or services may have serious consequences for national security".

In Bulgaria, however, critical infrastructure encompasses a system of facilities, services and information systems, whose disruption or destruction would have a

negative impact on the safety of people, the environment, the economy or the overall effective functioning of the Government.

In this context, of particular importance are several "institutionalized" attempts to define critical infrastructure. In one of those attempts, under the auspices of the European Union, it is stated that critical infrastructure is a "system or part thereof located in a Member State which is essential for vital societal functions, health, security, economic and social well-being and their destruction would have significant consequences in an EU Member State" (European Union Council Directive 2008).

This definition is strongly influenced by the 2001 terrorist attacks in the United States and the global war on terror following the 2004 terrorist attack in Madrid. All these developments led to the Initiative for the Adoption of "Communication for the Critical Infrastructure Protection in the Fight against Terrorism", outlining the proposals that Europe should take to prevent terrorist attacks of critical infrastructure, how to raise their resistance and to develop the ability to respond to potential attacks (Communication from Commission to the Council and the European Parliament-Critical Infrastructure Protection in the fight against terrorism, 2004).

Having in mind the example of the major terrorist attack in London in 2005, the Commission initiated and adopted the Green Paper on a European Programme for Critical Infrastructure Protection, which specifically focuses on the proposal for the establishment of a critical infrastructure protection programme. However, what makes the programme more current is its proposal to establish an information network for alarming in case of critical infrastructure threats. (Green Paper on a European Programme for Critical Infrastructure Protection, 2005). Furthermore, in 2006, the Commission adopted the European Programme for Critical Infrastructure Protection from all dangers, but it focuses on terrorism as a primary threat (Communication from the Commission on a European Programme for Critical Infrastructure Protection, 2006).

The next step of the European Union that deserves attention, and concerns critical infrastructure protection is the adoption of Directive 2008/114/EC on identification and designation of European critical infrastructure and the assessment of the need to improve their protection. According to this Directive, "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 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection)*.

In NATO, on the other hand, assets, services and information systems which are vital for a nation are considered critical and their destruction may endanger the security, economy, health, that is security of the nation in general or impede effective functioning of the states (Bognar, 2009: 552).

Lastly, we can draw several conclusions: the academic environment is making efforts to establish one acceptable definition of critical infrastructure, but there is still no universally accepted definition of the term critical infrastructure. Critical infrastructure is an asset, system, means, services, etc., which are vital for the normal functioning of the state in terms of economic, health, social and security needs.

Different national authorities have prepared a list of economic branches that are mentioned in the above definitions. In particular, they include water, food, energy, transportation, and priority is given to airports and railways, financial institutions, health, etc.

State governments are paying increasing attention to critical infrastructure. A positive example is the US government, the German government, and the UK government. These countries organize critical infrastructure equally at national, regional and local level. While poorly developed countries, for example, Croatia and Romania, deal with critical infrastructure exclusively at national level.

Hence, we can draw a general conclusion that the need for controlling and developing critical infrastructure is strongly expressed. In doing so, the emphasis should be placed on the goal of promoting institutional approach, aimed at creating a strategic framework for critical infrastructure.

1.2. Threats and risks to Critical Infrastructure

Contemporary societies nowadays face many threats and risks that go beyond the original framework of readiness and response to them and it is therefore necessary that the resistance and organization of the society be analyzed in the context of its static and dynamic characteristics. That is why Aristotle is right when he claims that the "whole is greater than the sum of its parts". We can apply this in the context of society's resilience to many threats and risks, since the society itself is a set of more specific complex systems interactively connected as a system (for example, infrastructure, health, energy, etc.). Namely, each of these separate systems has its own characteristics and dynamics, but when integrated into the social system, then they transfer from their own and become influenced by the characteristics of other systems. In other words, the essence of society is its complexity as a system built on complex internal and external relations and as a system that is constantly developing and adapting to the new future (Popovski, 2019: 45). Hence, that changed image can be described as a new security environment in which threats and risks are increasingly emerging from the non-military sphere of security and such a security environment becomes much more dynamic and uncertain, filled with challenges and dangers that impose the need for societies to offer comprehensive answer. For our analysis, it is important to note that the dramatic changes in the security environment, especially after the end of the Cold War, caused by the enormous distribution of threats and risks, have led to changes in the understanding and perception of protection and building a resistant society. In fact,

according to this, it is important to emphasize a few issues that, to a certain extent, influence risk management and in the direction of debates that have contributed to crystallizing what is nowadays called an extended and deepened approach to identify the so-called High Reliability Organizations that in fact constitute separate systems that are part of the social system, and which have continuous operation without errors, even in times of circumstances that are turbulent and dangerous (Roberts, 1990) and that can be identified e.g. as the air traffic control system (Weick, 1990) and health institutions (Chassin and Loeb, 2013), that is as part of the critical infrastructure. It is therefore important to emphasize that in a globalized and interdependent society, security is not only an attribute of the state and a result of the dynamics of the international security environment. It is therefore necessary for readiness to be understood in all its complexity from prevention to protection, from multi-sectoral approach in reducing risks and threats to critical infrastructure, to individual competence and responsibility of institutions, to provide the necessary normative, institutional and operational conditions for the establishment of critical infrastructure protection. This characteristic gives it a breadth, because in the context of the classification of threats and risks specifically for critical infrastructure, the contribution of Bognar (2009) is especially important, who, unlike in the past, lists several sectors such as economy, with particular emphasis on banking and finance, transportation (with special emphasis on airports and railways), distribution, energy, health, communications, utilities, food supplies, as well as key government services. The analysis shows that some of the critical elements in these sectors are not specifically "infrastructure", but a network or supply chains directly related to essential products and services. Therefore, the factors that threaten different elements of infrastructure are increasing, because critical infrastructure represents networks, facilities and systems distributed in space, whose continuity in work is influenced by numerous natural, technical and technological and anthropogenic factors. Regarding the aspect of protection, it is necessary to take into account the most significant threats and risks categorized in the abovementioned groups. On the other hand, special attention should be paid to the dependence and interdependence of the operation of critical infrastructure arising from the effects of the very nature, structure and business processes that affect critical infrastructure. It is therefore important to emphasize that different areas of the world have their own specific natural threats and risks that reiterate, interact with others and represent a potential and – or a direct threat to critical infrastructure. Studies prove that it is necessary to observe individual cost analyses and calculations to obtain a clear picture of threats and risks that, besides other values, endanger critical infrastructures. Therefore, Mikac (2017) is right in arguing that due to its geographical position, the area of Southeast Europe is a zone that is extremely vulnerable to natural threats such as floods, earthquakes and fires. In the last ten years, floods have been the biggest risk. From the technical and technological risks, it is necessary to mention disasters and major accidents in economic facilities; technical and technological disasters and major traffic accidents; nuclear hazards. Anthropogenic factors differ as well in the following way: acts related to terrorism, sabotage and crime. Thus, it is of particular importance to emphasize empirical evidence, so examples from the region of Southeast Europe and occasionally the wider context will be used.

1.2.1. Natural threats and risks to Critical Infrastructure

Natural threats to critical infrastructure include, but not limited to, the following: floods, fires, earthquakes, droughts, storms, and heat waves.

In their research, the United Nations state that the area of the Member States of the Organization for Security and Cooperation in Europe is very susceptible to natural disasters such as earthquakes, floods, droughts, storms, heat waves, wildfires. These threats have affected more than 76 million people in the last 25 years. By analyzing the precise data in the period from 1990 to 2014, storms (34%) and floods (31%) are most common natural disasters. According to them, floods (35%), storms (29%) and droughts (19%) affect most people in the area, and people have lost their homes mainly due to earthquakes (54%), floods (26%) and storms (16%). The aforementioned events in the past 25 years have resulted in the deaths of 182,075 people and economic losses of over trillion US dollars. (United Nations Development Programme, 2014: 8). Margareta Wahlström, Special Representative of the Secretary-General of the UN for Disaster Risk Reduction stated that, it is estimated that global annual economic losses caused by natural disasters are greater than $ 100 billion USD and trends show that it will continue to grow. According to Christian Friis Bach, UN Secretary-General of Economic Commission for Europe, annual losses caused by natural disasters amount to on average 10 billion Euro during the past 10 years in the European Union. This could include natural disasters in the European Union between 2002 and 2014 that caused more than 80 thousand deaths and more than 100 billion Euros in economic damages (European Commission, 2014: 1). Among numerous major natural disasters, statistically, floods represent the phenomena which very frequently and cumulatively cause great damage, economic and human losses, significant security and health challenges, numerous consequences for people, economy, critical infrastructure, service sector, environment and historical heritage (Mitrevska and Mikac, 2017: 28). Analyzes of the European Environment Agency's report for the period 1998 to 2009 point to the fact that 213 floods were reported in Europe, causing 1,126 deaths and economic losses of more than 52 billion Euros (European Environment Agency, 2011). Some areas in Europe are more flood prone than others, for example, for the past few years, floods have dominated the area of Central and South-Eastern Europe. In that sense, the analysis suggests that in the last ten years the historical maximum of the water has been noticed in the major European rivers such as the Danube, Tisza, Drava, Mura, Sava, and other rivers and their tributaries. It is particularly important to know that the floods caused multiple embankments breach, flooding of large protected areas, human casualties and massive damages to property in dozens of countries. Another European Commission's data worth mentioning is the hundred-year flood in Central Europe in 2013, i.e. a flood with the estimated probability to occur once in a hundred years, that have happened for the second time in only 13 years (European Commission, 2014: 1). In this context, it may be expected that more intensive and frequent floods will arise due to the effects of climate change and continued degradation of the environment (European Commission, 2014 *The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience).* In particular, a similar situation occurred in Southeast Europe, where the most significant consequences were manifested in 2014, that is, in the May floods

which is estimated to occur once in every 1000 years, and the most difficult areas were affected in Bosnia and Herzegovina, Serbia and Croatia. In all three states, 53 people died. In Bosnia and Herzegovina more than 1.5 million people were affected by floods, and more than 90,000 had to leave their homes. In Serbia, over 1.6 million people were affected by floods, and 31.000 were evacuated. In Croatia floods endangered 38,000 people (United Nations Development Programme, 2014). From the critical infrastructure aspect, these floods caused many problems in the functioning of the water supply system, transport and processing sector, agriculture, education and health system. Some flooded areas exhausted the local, regional, and even individual state capacities and resources and states received international assistance (Mitrevska and Mikac, 2017: 32). In this context, it is also very important to analyze the area of Southeast Europe, as part of the Mediterranean-transitional belt, which is characterized by a pronounced seismic activity. In that sense, this is especially valid for coastal areas and parts of the interior that had been affected by devastating earthquakes. Examples, which are often analytically exploited, relate to a number of very strong earthquakes that mark this area and the earthquake that occurred in 1667, with an intensity of 10 degrees according to the Mercalli-Cancani-Sieberg (MCS) scale, when Dubrovnik was almost completely destroyed and more than 3,000 people were killed (Government of the Republic of Croatia, 2009). The earthquake in Skopje in 1963, destroyed 75 to 80 percent of the city and caused more than 1,000 mortalities, more than 3,000 people were injured and between 120,000 and 200,000 people lost their homes. The 1979 earthquake in Montenegro, in addition to the Montenegrin area, caused casualties and material damages both in Croatia and Albania. In the earthquake, 101 people died in Montenegro, 35 in Albania, and more than 100,000 people lost their home. All of these examples, from the critical infrastructure aspect, mean significant damage, observed on numerous facilities, networks and systems of local and state infrastructure. Furthermore, major damages were caused in the educational, cultural, health, social and public administration facilities, in the economy, even to the extent that certain businesses completely ceased their activities.

Fires of a different kind pose a potential danger to all levels and forms of society because they potentially endanger a large number of people, assets in all types of facilities, in different modes of transport, tunnels, technological facilities and infrastructures that store hazardous goods. Here we could include open-space fires that have occurred in the last ten years in the area of Southeast Europe, in Bosnia and Herzegovina, Serbia, North Macedonia, and the interior of Greece.

Fires cause significant direct and indirect harm and their extinguishing sometimes requires engagement of large material, technical and human resources of the domicile states, cross-border cooperation and assistance as well as the activation of the European Union Civil Protection Mechanism to secure the necessary human and material capacities in order to be extinguished. They have direct consequences for certain critical infrastructure sectors such as: energy (production, including accumulation and dams, transmission, storage, energy and energy transport, distribution systems), traffic (road, rail, air, sea and river) and public services (provision of public order and peace, civil protection system, emergency medical assistance). Naturally, there are indirect consequences for other critical infrastructure sectors. (Mitrevska and Mikac, 2017: 34).

1.2.2. Technical-technological hazards to Critical Infrastructure

Threats of technical and technological nature can be caused knowingly or unknowingly, unintentional human error or a technological error. These include: traffic accidents, catastrophes, nuclear explosions, the release of biological agents that can cause massive infections, pandemics, and diseases affecting a large number of critical personnel (Bognar, 2009: 500). It is extremely important to understand that, among other things, the major technical and technological accidents and disasters inflict serious consequences to people, material and cultural goods, as well as to critical infrastructure. Namely, they can occur due to numerous reasons, but also as a domino effect after the initial accidents. From a theoretical point of view, the most general classification of major technical-technological accidents and disasters shows the full breadth of potential scenarios for endangering the values that need to be protected. The aforementioned are divided into: technical-technological disasters and major accidents in economic facilities; technical-technological disasters and major traffic accidents; nuclear risk. In particular, from the information gathered the production and storage of hazardous substances in numerous plants and warehouses is a constant risk of industrial accidents with catastrophic consequences. Globally, there are two well-known examples that marked this domain: the great disaster in Seveso in 1976 and the 1984 Bhopal disaster. The city of Seveso in northern Italy was the site of one of the greatest chemical accidents in the history of mankind. A large amount of dioxin was released from a chemical facility due to a technological failure. Approximately 2,000 people received medical attention, more than 80,000 animals were euthanized to prevent potentially harmful consequences for humans, about 1,800 hectares of soil was contaminated, and in the months following the accident, an increased number of spontaneous abortions was reported in the region. The biggest chemical disaster occurred in the Indian city of Bhopal when a large amount of chemicals leaked from a pesticide factory due to a technological failure. The consequences were horrifying. More than 25,000 people died and more than 150,000 people suffered serious illnesses and to this day, more often than elsewhere, children with severe physical and mental disabilities are born in that area. Seveso accident induced the European Union to strengthen business regulation and the control of chemical plants.

This was done through the Seveso Directive[1] which provides systematic control and monitoring of potential sources of danger from chemical pollution and harmful effects on the environment and people, which is also transparent to the general public.[2] The specificity of this approach regarding the consideration

1 The first directive called Seveso I was adopted in 1982. Seveso II was adopted in 1996 and took into account the disaster in Bhopal. Furthermore, Seveso III was adopted in 2012. Each new Directive has replaced the previous one and additionally tightened the regulation on the operation of chemical plants, which are currently over10,000 in the European Union.

2 For more infromation please see: The Council of the European Communities (1982) *Council Directive 82/501/EEC of 24 June 1982 on the major-accident hazards of certain industrial activities*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1982:230:FULL&from=EN; The Council of the European Union (1996) *Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01996L0082-20120813&from=EN;
The European Parliament and the Council (2012) *Directive 2012/18/EU of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC,* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018&from=EN, (cited 23 April 2017).

of critical infrastructure protection aspect is that we need as much transparency and publicly accessible indicators as possible for all processes in chemical plants, while on the other hand, the concept of critical infrastructure protection requires a certain level of confidentiality of data for the structure and process. When the legislator at the same time determines an obligatory plan to apply the Seveso Directive and will designate the plant as a facility of national critical infrastructure, the plant faces the challenges in the process of fulfilling both obligations, none of which is simple, and the application is a partial clash in the principles of action. (Mitrevska and Mikac, 2017: 36).

Experience shows that technical-technological disasters and major transport accidents (road, rail, air, sea and river) may arise due to the numerous processes that occur during the transport of dangerous substances. Possible causes of danger from unexpected events include: inadequate handling of vehicles in transport; unspecified cargo; defective parts for transport; inattention, neglect or negligence at work or improper handling; lack of process control; damage caused by mechanical impacts; device failure or errors when retracting and filling the container; fires in buildings; human deliberate activities for causing accidents USA (Sovacool, 2010: 369-400).

1.2.3. Anthropogenic threats and risks to Critical Infrastructure

Anthropogenic threats and risks to critical infrastructure include acts related to terrorism, abuse for political gain, abuse for economic gain, encouragement of armed conflicts, riots and protests, sabotage and crime aimed at the functioning of all or some parts of critical infrastructures.

Critical infrastructure is a huge, global sector and it is not possible to ensure its full protection at all times and in all places. Hence, it is likely that some terrorist attacks on critical infrastructure will succeed. Terrorists aim to spread fear, anxiety and panic, creating a perception that every citizen and critical node in the country's infrastructure is vulnerable to attack. There are many examples, for example the case of March 22, 2016, when two teams of ISIL operatives carried out simultaneous attacks in Brussels, at Zaventem airport (killing 11 people) and in the Maelbeek metro (killing 20 people). Around 300 people were injured (United Nations Security Council Counter-Terrorism Committee, 2017: 3-4). "Al-Qaeda" and its supporters have attacked facilities and personnel of oil companies in Algeria, Iraq, Kuwait, Pakistan, Saudi Arabia and Yemen, and have also captured many oil fields. The UN estimates that the income generated by ISIL from oil and petroleum products in 2015 was between $400 million and $500 million (United Nations Security Council, 2016). Although some authors note that energy attracts only a small fraction of terrorist attacks, the trend shows a rapid increase in interest of terrorists in oil and gas (Brookings Doha Center Analysis, 2016). According to numerous studies, more attacks worldwide are directed toward critical infrastructures (Mitrevska and Mikac, 2017: 37).

As critical infrastructure researchers point out, the next important anthropological threat is the act of sabotage, a borderline phenomenon between a terrorist act and a criminal act. According to them, the ranking of these attacks

is mostly aimed at infrastructures such as energy production and transmission systems, food and water supply networks, telecommunication networks, transportation networks, etc. Namely, it is continuously confirmed that the methods for committing such acts can be arson, explosions, use of weapons of mass destruction to the most common forms of attack, various cyber-attacks. However, it is equally important to have in mind that hostile cyber-actors come in both state and non-state variant and foreign intelligence agencies, terrorists, misguided activists, or simply individuals acting on their own can be pointed out as possible perpetrators. However, as technologies develop and become more complex, this also happens with the challenges for detection and protection against cyber-attacks. There are a number of indicators demonstrating that the main targets are high-technology industries, including the telecommunications sector, the oil and gas industry and other elements of the natural resources sector, the private sector, as well as universities involved in research and development. It is also known that State actors use cyber-attacks to disrupt political and economic activity as a means of influencing government decision-makers. Cyber-espionage threats, cyber-sabotage and other cyber-operations are part of a wider economic threat to key critical infrastructure sectors (Canadian Security Intelligence Service, 2017). Criminal activities toward critical infrastructure, however, are divided into insider and outsider activities. Insider threats are part of every organization and it happens most often when a trusted employee betrays his obligations and loyalty to the employer by sabotage or espionage against them. Specifically, "insider betrayals" can be the acts of theft as subtle forms of sabotage or more aggressive acts like violence at the workplace. The threat that the insiders represent is a term that is commonly used in case of abuse of the IT network. This often leads to further confusion about the nature and severity of the threat (Noonnan and Archuleta, 2008). External threats are various attempts to infiltrate the system, either physically or through the Internet and the motive may vary depending on the attacker's motivation. In particular, physical incursions constitute an attempt to alienate part of the equipment or obtain important information directly through collaboration with company employees or with a certain type of fraud or extortion, to attack cyberspace with invasion. Hence, such attacks on critical infrastructure occur every day on a global scale and unfortunately, their trend is constantly increasing. That is why it is argued that cyber space and critical infrastructure have become inseparable. Security challenges are emerging as well as consideration what is the best way to protect vital parts of critical infrastructure from external intrusion this strong correlation between the Internet and critical infrastructures comes at a cost of increased complexity and, as a consequence, increased risks of accidental faults.

1.3. The need for Critical Infrastructure Protection

In contemporary conditions, the understanding and application of critical infrastructure protection is strongly influenced by several factors such as the complexity of critical infrastructure, competence regulation, lack of accountability in sectors, where above all a number of state and private institutions are engaged, which, on the other hand, increases vulnerability and directly affects the effective approach to critical infrastructure protection, the quantum of knowledge and skills

in relation to critical infrastructure protection and interdependence of the critical infrastructure sectors, etc. (Prezelj, 2008: 13). Therefore, the authors conclude that the critical infrastructure protection is a very broad and dynamic activity and is accomplished in two different ways. The first is carried out by public bodies, such as various legislative institutions, law enforcement agencies, inspection and judicial authorities and private security organizations. The second are the activities carried out by international bodies such as the European Union and NATO. Other theorists, in a similar way, argue that each case is unique, therefore it is necessary to pay special attention to the fact that many actors participate in the critical infrastructure protection in different stages and processes. Mikac, the advocate of this thesis, believes that in order to illustrate the level of discussion on this issue, it is necessary to provide examples of critical infrastructure: 1.) Energy Sector – nationally important oil and gas refineries; 2.) Transport Sector – the largest airports; 3.) Information and Communication Sector – the most important databases of each country; 4.) Economic Sector – National Central Bank systems; 5.) Health Sector – Clinical Hospital Centers; 6.) Food Sector – grain storage silos; 7.) Water Management Sector – wellfields; 8.) Sector for production, storage and transport of hazardous substances – integrated monitoring and control system for transport of hazardous substances; 9.) Public Services – Emergency Medical Assistance; 10.) Tourism Sector – national monuments that are the reason for the arrival of many tourists (Mitrevska and Mikac, 2017: 35). Hence, a common view is that it is obvious that critical infrastructure is very diverse and is represented in networks, facilities and systems that are not always physically visible, but consist of many components and interdependencies, most often in the Cyber world. The reasons for this are different. We can point out the example with the National Bank building, which as a building itself is not a critical infrastructure, but the structures and processes that take place within the building are. For that matter, we are again making an additional breakdown and we have to determine which processes are irreplaceable, whether there is an alternative to their action and what will happen if they stop or temporarily cease to operate. Furthermore, in an effort to elaborate the need to protect critical infrastructure, one should bear in mind that they are complex systems that require a holistic approach in considering their functioning, with an emphasis on the sources of their internal and external threats, the importance for the sector itself and dependence and interdependence with other sectors and critical infrastructures, strengthening their resistance and their protection.

Regarding the description of the situation and what should be done, there is a basic position according to which the overall protection of the state and society from the aspect of preserving the functioning of critical infrastructure must be based on the „protection package" of all infrastructures as well as of each individual. At first glance, such approach leads to the conclusion that each infrastructure and the entire country will be best protected if the supply and delivery routes alter, as much as possible, to create and strengthen alternatives to critical infrastructure and strengthen their resilience. In fact, such buildings will be protected if they are built in areas where there is the least risk of flooding, fires and earthquakes. If this is followed by construction, obliging the rules of the profession and using quality

materials, respecting all construction and maintenance standards, then it is clear why the protection package will be more efficient and effective. In addition, the next step is equally important, and that is to create a complete accompanying documentation and knowledge, in order to avoid standstills and domino effects. However, one should bear in mind the general impression that there is resistance of the system itself, its robustness and high functionality. The analysis of the question whether the realization of critical infrastructure protection through the prism of all the necessary assessments, analyses and plans required by other laws which depend on national laws that are directly related to the issue of critical infrastructure, is only an upgrade to everything that has been previously done. The analysis of the need to protect critical infrastructure is a good example to indicate that there is a full range of required and previously undertaken activities through which the vulnerability of critical infrastructure can be avoided and reduced with structural measures. In particular, there are numerous indicators that there is a very wide range of jobs and areas of responsibility, with a clear definition of institutions, with clearly defined programs and work procedures competent for critical infrastructure protection.

1.3.1. Organization of Critical Infrastructure Protection

The theory and practice is dominated by the view that the approach to critical infrastructure protection should be primarily based on risk analysis while clearly outlining which risks jeopardize the operation of critical infrastructure and how to respond to them. Some authors suggest the risk analysis to refer to the processes used to assess those probabilities and consequences, as well as to study how to incorporate the assessments made in the decision-making process. The second proposal is the risk assessment process, serving as a decision-making tool, with its results being used to provide guidance on the most-at-risk areas and to devise policies and plans to ensure that systems are adequately protected (Myriam, 2006: 2).

Similar attention to this organizational approach to the implementation of critical infrastructure protection is also being devoted in the European Union and the countries that aspire to full membership (as is the case of the Republic of North Macedonia) and this is implemented in the *Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (Council of the European Union, *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*). Thus, the Introduction in the Directive clearly indicates that the primary and key responsibility for the protection of European critical infrastructures lies with the Member States and the owners/operators of such infrastructures (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 6). This principle also applies to the protection of the national critical infrastructure. On the other hand, from the aspect of cooperation between the public and the private sector, the provision of the Introduction to the Directive is very significant, which states how the involvement of the private sector in overseeing and managing risks, business continuity planning and post-disaster recovery, the community approach, should

encourage full involvement of the private sector (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 8).

However, as some authors note, the Directive states that in the organization of critical infrastructure protection it is necessary to have three important components: to make operational security plans; appoint Security Liaison Officers and nominate contact points for critical infrastructure protection. Operator security plans or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritization of counter measures and procedures should be in place in all designated critical infrastructures. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated critical infrastructures possess relevant Operator security plans or similar measures. Where such plans do not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the establishment of Operator security plans (Council of the European Union, *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, paragraph 11). Security Liaison Officers should be identified for all designated critical infrastructures in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated critical infrastructures already possess a Security Liaison Officer or equivalent. Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 13).

Effective protection of critical infrastructures requires communication, coordination, and cooperation at national level. This is best achieved through the nomination of critical infrastructure protection contact points in each Member State, who should coordinate critical infrastructure protection issues internally, as well as with other Member States and the Commission (Council of the European Union, Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, paragraph 17). Thereafter, a three-step process precedes the immediate implementation of critical infrastructure protection: 1.) Identification; 2.) Determination; 3) Protection. Identification of the potential critical infrastructure is conducted by sectoral holders (competent ministries) in cooperation with regulatory agencies. Once these stakeholders identify the potential critical infrastructure within their sector, they compile the list and submit it to the government for confirmation. In the next step, the government reviews the proposed lists of potential critical infrastructures, and decides, with a decision, on an individual critical infrastructure

or all the proposed ones. That decision is then delivered to the owner or manager of the critical infrastructure and to the relevant ministry or regulatory agencies. Upon receipt of the decision, all the above mentioned actors are obliged to communicate and cooperate with each other. The first level of cooperation is to see if there is an Operator security plan and whether it is adequate for the desired level of critical infrastructure protection. It is also necessary to appoint and mutually connect Security Liaison Officers who will carry out subject tasks between the relevant ministry, critical infrastructure, regulatory agencies, as well as cooperate with other stakeholders in this process and the critical infrastructure protection system. As far as protection steps are concerned, this is done in accordance with the Operator security plan, which must be set up according to four basic principles of crisis management: prevention, preparedness, reaction and recovery. The abovementioned plan must evaluate the analysis of the business risk of the critical infrastructure, its threats, the response force, cooperation with the competent institutions, the implementation of protection measures, the scenario of possible and worst-case event or more of such events that may occur in the critical infrastructure. In addition, it must contain a communication plan as well as an address book of the most important contacts.

Within the Critical Infrastructure Protection System, each country independently determines the organization and implementation of all processes and the level of the actors involved. There is no universal form to follow when establishing the system, but there are certain principles outlined above which should be respected so that the system is more efficient, more cost-effective and self-sustaining (Mitrevska and Mikac, 2017: 42).

1.3.2. Institutions competent for Critical Infrastructure Protection

There are two basic approaches to the orientation of the level of determining critical infrastructure. The first approach concerns territorially smaller countries where critical infrastructure is only determined at the national level and the system is simpler for coordination since the relevant bodies of regional and local self-government units are not involved in the processes. While the second approach is presented by larger countries where critical infrastructure is determined at national, regional and local level.

From the analysis of the institutions that are competent for critical infrastructure protection, we emphasize the role of the government of each state, which should be included in the system of critical infrastructure protection for several reasons. Firstly, the Government is a proposer of laws and by-laws. Secondly, it has the opportunity to give authority to certain ministries and/or central government bodies to be coordinators of the entire system and holders of sectoral processes. Thirdly, the Government provides a strategic framework that is essential for the successful functioning of the system and cooperation, communication and coordination of all involved actors. Fourthly, the Government has the power to determine the sectors from which central government bodies identify certain critical infrastructures in order to ensure a holistic approach to protecting and reducing adverse impacts in the event of a threat to critical infrastructures.

As the next most important actor competent to protect critical infrastructure we highlight the role of the *coordinator* of the entire critical infrastructure protection system. There are various examples and practices on which body is appropriate for this role, for example in the United States, this function is performed by the Ministry of Homeland Security. While in most European countries, the function is assigned to the Ministry of the Interior. However, there are examples, such as that of the Republic of Slovenia, where the Ministry of Defense has that duty, or the Republic of Croatia, where it is assigned to the National Protection and Rescue Directorate (an independent central state level body under the ministries). The role of the system coordinator is to communicate directly with all actors of the system, with international actors, to submit reports to the Government and most often represents their country at coordinative meetings organized by the European Commission. The mentioned institution, in cooperation with the competent central authorities of the state administration within the scope of which is the individual critical infrastructure, constantly monitors and assesses the threats and proposes operational and other measures for assessing the criticality and the need for the proposed measures for the management and protection of critical infrastructure.

The next important actor competent for critical infrastructure protection is within the *central state administration bodies* appointed by the Government, most often the relevant ministries responsible for the implementation of sectoral policies. These institutions, in cooperation with the competent regulatory agencies, are responsible within their scope for identification (determination) of specific systems or their components as critical infrastructures, ensuring critical infrastructure management and their protection. As an example, we will mention the energy sector. The competent institution is predominantly the Ministry of Economy (or the Ministry of Energy in some countries), which provides sectoral policies for the development of relevant sector, cooperates, communicates and takes care of the business of all actors on the market, carries out supervisory oversight, paying special attention to the areas of sectoral critical infrastructure and their sectoral dependence and interdependence with critical infrastructures in other sectors. There is a presumption that depends on the development of the state, that all sectors do not have established regulatory agencies. However, as the energy sector is one of the most critical sectors of critical infrastructure, all countries have established energy regulatory agencies. These agencies have public authority and their activities include: issuing, extending and transferring licenses for carrying out energy activities and temporarily and permanently revoking of permits; supervision of energy entities in performing energy activities; supervising the management of business books; overseeing the principle of transparency, objectivity and impartiality in the work of the energy market operators; issuing a decision on acquiring the status of a qualified energy producer and revoking the said decision; issuing or approving energy prices; cooperation with international regulatory agencies, etc. Identification of infrastructure criticality is, as a rule, made for each system, network and infrastructure facility within the competence of the central body of the state administration, in which the relevant ministry and the regulatory agency collaborate (or more of them if present in the particular sector). Criteria for assessing the criticality of the infrastructure can be: life and

health – determining the impact of disruption and/or interruption of work on life and health; the timeframe – in case of disruption/interruption of work, it will be determined how long this disruption/interruption of work will have consequences on total business/service delivery (in a shorter time, greater criticality); scope – determines how much the total product and/or service will be affected in the event of a disruption or complete termination of work; legal, regulatory and contractual significance; economic/financial damage. (Mitrevska and Mikac, 2017: 43).

Then the next actor is *the owner or manager* of the critical infrastructure. They are directly responsible for the management and critical infrastructure protection in all conditions. They need to make a risk analysis as the basis for creating an Operator security plan. In developing risk analyzes, they collaborate with central state administration bodies, whose scope is critical infrastructure, competent regulatory agencies, and the central state administration body, which is the coordinator of the overall system. The Operator security plan also identifies those entities responsible for critical infrastructure protection at all stages and alongside with law enforcement agencies, play a major role for companies that provide private security. The challenge that is present everywhere in the world is to provide information exchange, especially to those which are sensitive, so owners/managers can be aware of whether they are endangered. Directive 2008/114/EC itself recognizes aforementioned and specifies that critical infrastructure owners/operators should gain access to best practices and methods related to critical infrastructure protection, primarily through the relevant bodies of the Member States, and that the exchange of information should take place in conditions of trust and security. Information sharing requires a trusted relationship in which companies and organizations know that their sensitive and confidential data will be sufficiently protected. This is the most complex part of the critical infrastructure protection arrangement and an indicator for the general development of society and the state. (Mikac, 2017: 44).

1.3.3. Critical Infrastructure Protection through Public-Private Partnership

Critical infrastructure theorists agree that when protecting critical infrastructure, the public and private sector should have a special place. However, some authors also add additional arguments, starting from the definition that public-private partnership is a joint initiative of the public and private sectors where each entity contributes to the specific system resources and participates in planning and decision-making (White House, 1998). In particular, the first argument suggests that public-private partnership systems should aim at strengthening the resilience and critical infrastructure protection. The second argument points out that with increased awareness of the importance of critical infrastructure protection for everyday functioning of all entities, national security and international cooperation, as well as the exchange of knowledge, experiences and best practices between the private and public sectors, aims at directly affecting an increase of resistance and critical infrastructure protection system.

Theorists point out that in practice the creation of a proper system of critical infrastructure protection is a very difficult task for any country at any stage

of development. The general conclusion is that threats and systems become more complex and endanger the functioning of infrastructures which is a major challenging for the state. But, as we will see in the elaboration of the other Chapters through the examples of Croatia and the United States, it becomes evident that each country has its own approach to critical infrastructure protection, depending on the degree of private ownership in companies, the stability of the state structure or past experiences. The general conclusion is that it will take some time for the states to accept public-private partnership in protecting critical infrastructure, in the full sense, as an indispensable and necessary concept for developing and improving business and service levels. The best example of this are the countries of Eastern and Southern Europe. Hence, it is necessary to stimulate and establish an appropriate and country specific system of public-private partnership in the field of critical infrastructure protection. Several types of solutions are offered for this need: it is necessary to obtain the widest possible participation of proposals, it is important to ensure an adequate level of awareness, clearly define the powers and responsibilities at the level of the very critical infrastructure operators, and the exchange of information (information essential to the provision of national security and information that in the business environment represent important business data, which can reduce the competitive advantage of the company managing critical infrastructure). Furthermore, it is necessary for public-private partnership to focus on certain elements of success and sustainability of cooperation in order to implement the objectives of resilience and protection of critical infrastructures, such as:

- **Defining roles and responsibilities.** In particular, public-private partnership should regulate the obligations and rights of public and private partners while respecting the basic principles in the preparation and implementation of public-private partnership projects, i.e. the principle of public procurement, the principle of public interest and the principle of cost effectiveness.
- **Application of resources**. This is aimed at reduction of criticality and/or increased flexibility of infrastructures, where public private partnership stakeholders should include the resources at their disposal. Also, in addition to the existing public and private financial resources, it is necessary to plan the possible use of European structural and investment funds to support public-private partnerships in protecting critical infrastructure.
- **Openness for capacity development and changes** applies when there is a need for institutional changes in the process of critical infrastructure risk management at the level of the service provider or bodies.
- **Realistic expectations** refer to short-term plans with limited time frames that result in solutions which are difficult to implement. Therefore, it is not realistic to expect that the involvement of the private sector over a short period of time shall compensate for the shortcomings in terms of the resources or activity of public institutions in general (RECIPE, 2015).

Based on public-private the private sector generally delivers a high level of quality and service and should therefore be recognized as a trusted partner by competent public authority and by the owner/manager of critical infrastructure.

For example, at the EU level there is still no comprehensive set of measures to regulate the activities for critical infrastructure protection from the private sector, and jurisdiction is within the domain of national legislation. On the other hand, there are separate ISO standards for protection of private security services that need to be considered and implemented in the private sector's work before entering the field of critical infrastructure protection.

These are numerous indicators that point out that this must be taken into account when it comes to building an effective system for critical infrastructure protection.

1.4. Indicative list of Critical Infrastructure

A precise specification of critical infrastructures has been established within the EU. For instance, the Indicative List of the European Commission includes: energy, information and communication technologies, water, food, finances, public administration, transportation, chemical industry, etc. (Green paper on a European Programme for critical infrastructure protection, 2005: Annex II).

In addition, a precise specification of critical infrastructures has been established in most NATO Member States. For example, in *Germany* it includes: energy, telecommunications, information infrastructure, public health, food and water supplies, banking, finances, transportation, emergency and rescue services, government institutions, police, customs, armed forces, etc.

In *France,* the list includes the state sector (civilian activities, law and military activities), the needs of people (food, water, health), the economy (energy, trade and finance), technologies (industry, communication technologies and broadcasting) (Ducamin, 2016: 5).

In the *United Kingdom,* it includes energy, telecommunications, government institutions, health, finances, transport, emergency services, water and drainage systems, etc.

In *Sweden,* it includes energy, transport, water and municipal services, food, healthcare, information and communication, emergency services, industry and commerce, financial services, government, and social insurances.

In the *United States,* it includes energy, information, telecommunications, public health, food, water, finances, emergency assistance, government institutions, basic defense industry, chemical industry and hazardous substances, etc

In *Croatia,* the list refers to transport (land, rail, air, sea), energy (electricity, gas, oil and petroleum products), communications and information technologies.

Slovenia identifies, recognizes and determines the critical infrastructure using the identification criteria (published in 2012 as Basic and Sectoral Criteria for Designating the Critical Infrastructure of National Importance for the Republic of Slovenia and the **Amendments** of 2014). Basic criteria have been differentiated, as follows:

- A critical infrastructure that can cause death of more than 50 people due to interruption or disturbance of work.

- A critical infrastructure that, due to dysfunction, can affect human health to such an extent that it will be necessary to hospitalize more than 100 people for more than a week.
- A critical infrastructure that, due to interruption or violation of the order of work and services, causes damage or destruction of facilities or areas affecting the national security of the Republic of Slovenia and to that extent aggravating the implementation of national security, internal security and protection from natural and other disasters.
- A critical infrastructure that, due to dysfunction, affects the implementation of economic and other activities, leading to a disruption in the supply of drinking water or food for the population of over 100.000 people for more than a week.
- A critical infrastructure that, due to dysfunction, affects the interruption of power supply for three days or more than a week for over 100.000 people.
- A critical infrastructure that, due to dysfunction, affects the disruption of the supply of petroleum products for more than a week for over 100.000 people.
- A critical infrastructure that, due to dysfunction, causes great damage due to water impact and endangers habitats and soils in an area of over 100 hectares.
- A critical infrastructure that, due to dysfunction, causes information or communications disruptions in supporting the operation of another critical infrastructure for up to 24 hours.
- A critical infrastructure that, due to dysfunction, causes significant consequences in other countries, in accordance with previous criteria (Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012: 1-2).

In addition, criteria have been adopted for each of the eight critical infrastructure sectors: energy, transportation, food, drinking water, health services, finance, environmental protection, communications and information technologies. These criteria are shown in Table 1.

TABLE 1:
List of Critical Infrastructure Sectors in the Republic of Slovenia

Sector	Criteria
Energy	• Decay of the energy system on the territory of the Republic of Slovenia which takes more than 7 days to rehabilitate. • A disruption of electricity supply for three days for over 100.000 people. • Interruption in the supply of petroleum products and natural gas for more than a week in the volume of over 100.000 people and costs in the amount of 10.000.000 Euros per day.
Transportation	• Disabling rail traffic on key routes for more than a couple of weeks and damages of 10.000.000 Euros per day. • Disabling air traffic in the Republic of Slovenia for more than 12 hours.
Food	• Unable to provide the basic food products for a week for over 100.000 people
Drinking water	• Unable to provide drinking water supply for a week for a population of over 100.000 people.
Health	• Unable to provide emergency care and public health services for over 100.000 people.
Finance	• Unable to provide money supply for more than 3 days in an area of more than 50.000 people. • Failure to operate state finances for more than 7 days. • Non-functioning payment operations for more than 1 day.
Environmental protection	• Causes of pollution with short harmful effects on the health of the population in an area of over 50.000 people.
Communications and Information Technologies	• Failure of communication equipment, network and services vital for the key functions in the country and the work of several sectors of critical infrastructure, national security system, the electricity sector and finances for more than 6 or 24 hours.

Source: Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012: 2-3.

Republic of North Macedonia has no formally defined list of critical infrastructure, it is legally unregulated and there is no identification and protection of critical infrastructure. Hence, the EU's precise specification of critical infrastructures and the stated solutions in the EU and NATO Member States from which we would single out the examples of Slovenia and Croatia, will be of great benefit to the future activities in creating a formal framework for national critical infrastructure protection.

1.5. Standard for Critical Infrastructure Protection

Comparatively observed, there are certain differences in the standardization of the framework for critical infrastructure sectors between the European Union and the United States. However, apart from these differences, effective standards for critical infrastructure protection are the cornerstone of any successful program for critical infrastructure protection. Critical infrastructure protection standards and norms include a risk assessment methodology that is necessary to identify threats, vulnerability assessment and impact assessment of assets, infrastructure or systems taking into account the likelihood of their occurrence. There is a significant number of methodologies for risk assessment of critical infrastructures. In general, the approach that is used is fairly common and consists of several main elements. Firstly, identification and classification of threats, identification of vulnerability and impact assessment. This is a well-known and already established approach for risk assessment and represents the elements of almost all risk assessment methodologies. However, there is a big difference in methodologies for risk assessment based on the scope of the methodology, the target population (policy makers, decision makers, research institutes) as well as their domain of applicability (level of means, infrastructure/system level, etc.).

Generally speaking, standards play a major role in defragmenting markets and help the industry to reach certain economic values. The standards are also of great importance to the demand side, especially with regard to the interoperability of the technologies used by the first accountable persons, law enforcement agencies, etc. Additionally, the standards are essential to ensure uniform quality in providing a secure service. Creation of the EU standards and their promotion on a global level is also a vital component of the global competitiveness of the EU security industry. However, several EU standards exist in the security sphere. It seems that different national standards represent a major obstacle to creating a genuine internal security market, which hinders the competitiveness of the EU industry. The European Commission has already announced in its message on strategic vision for European standards, stressing the need to accelerate standardization efforts in the security sector. Therefore, by issuing the document M/487 of the Commission, in 2011 authorized European Standardization Organizations (CEN, CENELEC and ETSI) to make a detailed overview of the existing international, European and national standards in the security area, as well as to establish a list of gaps in the standardization and to propose a creation of standardization program. The mandate was accepted by the European Standardization Organizations. The work was assigned to CEN/TC 391 "Social and Civil Security" whose secretariat is managed by a Dutch Institute for Standardization (NEN). There are several common threats (mandates) from the report and can be summarized as follows:

- Confidentiality – special attention is needed to standardize security.
- Integrity on behalf of all stakeholders.
- Risk-based work – ISO 31000 is a widely accepted standard in the sector.
- Terms and definitions –clear definitions are needed.
- Standardization and innovation – innovation can benefit greatly from early standardization.

- Proposals for the timeframe should be priority and the roadmap is just the beginning of development.
- EU Policy – standardization in the security sector is an excellent tool to support the EU policy.
- Stakeholder responses – stakeholders were generally positive about the mandate and participated actively.
- The need to meet the EU objectives and criteria by review from experts.

The standards, best practices and guidelines drawn from the European Reference Network for Critical Infrastructure Protection (ERNCIP) are most commonly repeated. The inventory is subdivided according to representative thematic areas and sectoral criteria such as Authentication and Biometry, cross sectoral, detection of explosives, IT and cyber security, resistance to structures from explosives, traffic safety and water and the environment. The most representative standards for each of the above-mentioned thematic areas are the following:

A. Water & Environment

- ISO 15839:2003 Water quality -- On-line sensors/analysing equipment for water - Specifications and performance tests;
- ISO 24510:2007 Activities relating to drinking water and wastewater services -Guidelines for the assessment and for the improvement of the service to users;
- ISO 24511:2007 Activities relating to drinking water and wastewater services -Guidelines for the management of wastewater utilities and for the assessment of wastewater services;
- ISO 24512:2007 Activities relating to drinking water and wastewater services - Guidelines for the management of drinking water utilities and for the assessment of drinking water services.

B. Transport Security

- PAS 68 Impact test specifications for vehicle security barriers;
- ASTM F2656 - 07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers;
- CWA 16221:2010 Vehicle security barriers. Performance requirements, test methods and guidance on application;
- BS EN 1317-1:2010 Road restraint systems. Terminology and general criteria for test methods;
- BS EN 1317-2:2010 Road restraint systems. Performance classes, impact test acceptance criteria and test methods for safety barriers including vehicle parapets;
- BS EN 1317-3:2010 Road restraint systems. Performance classes, impact test acceptance criteria and test methods for crash cushions;

- DD ENV 1317-4:2002 Road restraint systems. Performance classes, impact test acceptance criteria and test methods for terminals and transitions of safety barriers;
- NCHRP Report 350 Recommended Procedures for the Safety Performance Evaluation of High way Features;
- BS EN 12767:2007 Passive safety of support structures for road equipment. Requirements, classification and test methods;
- PAS 69:2006 Guidelines for the specification and installation of vehicle security barriers;
- ISO 13492-2007 Download ISO 13492-2007 Financial services-Key management related data element-Application and usage of ISO 8583 data elements 53 and 96;
- ISO 22902-2:2006. Road vehicles -- Automotive multimedia interface -- Part 2: Use cases;
- ISO 28000:2007 Specification for security management systems for the supply chain;
- ISO/TS 10891:2009, Freight containers - Radio frequency identification (RFID) - Licence plate tag;
- ISO/IEC 9797-2:2011, INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES - MESSAGE AUTHENTICATION CODES (MACS) -- PART 2: MECHANISMS USING A DEDICATED HASH-FUNCTION;
- ISO 11064-4:2013, ERGONOMIC DESIGN OF CONTROL CENTRES -- PART 4: LAYOUT AND DIMENSIONS OF WORKSTATIONS;
- ISO/PAS 16917:2002. Ships and marine technology -- Data transfer standard for maritime, intermodal transportation and security.

C. Authentication and Biometry

- BSI TR-03104 Technical Guideline for production data acquisition, -quality testing and transmission for official documents;
- BSI TR-03105 Conformity Tests for Official Electronic ID Documents;
- BSI TR-03121 Technical Guideline Biometrics for Public Sector Applications;
- BSI-TR 03132 Technical guidelines and protection profiles regarding electronic ID documents.

D. Information Technology and Cyber Security

- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements;
- ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management;
- ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management;

- ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements;
- ISO 9241-110:2006 Ergonomics of human-system interaction -- Part 110: Dialogue principles;
- ISO 9241-11:1998 Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability;
- ISO/IEC DIS 25051 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing;
- ISO 9241-210:2010 Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems;
- BS EN 45011:1998 General requirements for bodies operating product certification systems;
- NIST HANDBOOK 150-17 National Voluntary Laboratory Accreditation Program;
- IEC 60870-5-104 Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles;
- IEC 61850-SER ed1.0 Communication networks and systems in substations;
- NIST IR 7628 Guidelines for Smart Grid Cyber Security
- NIST 800-53 rev3
- ISO 22311:2013 Video surveillance export interoperability
- IEC 62676-2:2013 Video surveillance for the use in security applications.

E. Resistance of Structures to Explosives

- DIN EN 13541:2012 Glass in building - Security glazing - Testing and classification of resistance against explosion pressure;
- DIN EN 14449:2005 Glass in building - Laminated glass and laminated safety glass - Evaluation of conformity/Product standard;
- ISO 16934:2007 Glass in building -- Explosion-resistant security glazing -- Test and classification by shock-tube loading;
- DIN EN 13123-1:2001 Windows, doors and shutters - Explosion resistance; Requirements and classification - Part 1: Shock tube; English version of DIN EN 13123-1;
- DIN EN 13124-1:2001 Windows, doors and shutters - Explosion resistance; Test method - Part 1: Shock tube; English version of DIN EN 13124-1.

F. Explosive Detection

- ECAC Common Evaluation Program for Security Equipment - Explosive Detection System;
- ECAC Common Evaluation Program for Security Equipment - Liquid Explosive Detection;
- ECAC Common Evaluation Program for Security Equipment - Security Scanners.

G. Cross Sectorial

- ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories;
- ISO 14001:2004 Environmental management systems -- Requirements with guidance for use;
- ISO 22301:2012 Societal security -- Business continuity management systems – Requirements;
- EN 14383- 1:2006 Prevention of crime-Urban planning and building design – Part 1: Definition of specific terms. (Paustourli and Kourti, 2014)

Chapter conclusion

Bearing in mind the foregoing, one can conclude that there is still no universally accepted definition of the term "critical infrastructure". This can be seen in numerous definitions of "critical infrastructure" in literature. Different countries define critical infrastructure in different ways. Nevertheless, most often, everything comes to that that infrastructure, systems and resources are of vital importance for a society. Starting from the need to provide the vital functions of the state, there is a possibility to determine the significance of criticality of certain infrastructure, because it is closely related to energy security, telecommunications, energy systems, gas and oil pipelines, the economy, transport, water supply, etc. In this context, it should be emphasized that "critical infrastructure" encompasses resources that are necessary for the functioning of societies, such as: energy facilities and networks, communication and information technology, finance, health, food, water, transport, production, storage and transport of hazardous substances and government facilities. The protection of critical infrastructure, such as water, energy and telecommunications, is of the utmost importance. If these systems are at risk, that is, in deficit or destroyed, there will be an impact on the economy, the psychology and security of the nation, that is, of the society. The high interdependence of these systems with other systems of social life, requires more attention to their protection. The need for critical infrastructure protection basically stems from the need for each country to have a systematic approach to the existing infrastructure and it is necessary to define the infrastructure as critical, due to the possibility to be a potential target. There are many different solutions and practices, but each country should recognize the most appropriate model for critical infrastructure protection on its own. Therefore, it is necessary to regulate critical infrastructure protection through an integrated approach, starting from identifying, preventing and preparing to deal with threats to critical infrastructure, and by reducing the vulnerability of critical infrastructure to mitigate the consequences on critical infrastructure. In parallel with the determination of strategic imperatives, it is also necessary to provide a good assessment of threats, vulnerability, indicative list and standards for critical infrastructure protection and on the consequences to critical infrastructure, and above all, to improve the resilience of critical infrastructure, that is, safe critical infrastructure from possible human, physical and cyber threats.

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