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

Prof. d-r Marina Mitrevska
Prof. d-r Toni Mileski
Doc. d-r Robert Mikac

**CRITICAL INFRASTRUCTURE:
CONCEPT AND SECURITY CHALLENGES**

Reviewer:
Prof. d-r Setola Roberto
Prof. d-r Jonas Johansson

Publisher: Friedrich Ebert Foundation, office Skopje
Translate: d-r Vesna Tasevska-Dudevska
Printing: Kontura
Copies: 50

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

355.45(497.7)
355.45(100)

MITREVSKA, Marina
Critical infrastructure : concept and security challenges / Marina Mitrevska, Toni Mileski, Robert Mikac. - Skopje : [Friedrich Ebert Stiftung - Office Skopje], 2019. - 174 стр. : табели, граф. прикази ; 25 см

Фусноти кон текстот. - About authors: стр. 173-174. - Библиографија: стр. 159-162. - Регистар

ISBN 978-9989-109-93-5
1. Mileski, Toni [автор] 2. Mikac, Robert [автор]
а) Критична инфраструктура - Државна безбедност - Македонија COBISS.MK-ID 111119370

The views expressed in this publication are not necessarily those of the organization for which the authors work.

MARINA MITREVSKA
TONI MILESKI
ROBERT MIKAC

CRITICAL INFRASTRUCTURE: CONCEPT AND SECURITY CHALLENGES

Skopje, 2019

Content

List of Abbreviations

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
BS	British Standards
CEN	Comité Européen de Normalisation (French) – European Committee for Standardization
CENELEC	Comité Européenne de Normalisation Électrique (French) – European Committee for Electrotechnical Standardization
CEPS	Central European Pipeline System
CI	critical infrastructure
CIP	critical infrastructure protection
CIPP	Critical Infrastructure Protection Plan
CIWIN	Critical Infrastructure Warning Information Network
CPNI	Centre for the Protection of National Infrastructure (United Kingdom)
CSDP	Common Security and Defence Policy
DHS	Department of Homeland Security
DIN	Deutsches Institut für Normung (German) – German Institute of Standardization
DOT	Department of Transportation
ECAC	European Civil Aviation Conference
ELEM	Macedonian Electric Power Plants
EO	Executive Order
EPA	Environmental Protection Agency
ERNCIP	European Reference Network for Critical Infrastructure Protection
ETSI	European Telecommunications Standards Institute
EU	European Union
FINRA	Financial Industry Regulatory Authority
GAO	Government Accountability Office
G-8	Group of eight – Forum of governmental leaders of eight large and industrialized nations
HIPAA	Health Insurance Portability and Accountability Act
IEA	International Energy Agency
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
ISC	Interagency Security Committee

ISIL	Islamic State of Iraq and the Levant
ISO	International Organization for Standardization
IT	Information technology
JSC MEPSO	Macedonian Electricity Transmission System Operator
MCS	Mercalli-Cancani-Sieberg
MI5	Military Intelligence, Section 5 (United Kingdom domestic intelligence agency)
MSB	Myndigheten för samhällsskydd och beredskap (Swedish) – Swedish Civil Contingencies Agency
NATO	North Atlantic Treaty Organisation
NCISAC	National Council of Information Sharing and Analysis Centers
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPR	National Preparedness Report
NPRD	National Protection and Rescue Directorate
OSCE	Organization for Security and Co-operation in Europe
PCCIP	President's Commission on Critical Infrastructure Protection
PPD	Presidential Policy Directive
RC3	Regional Consortium Coordinating Council
RECIPE	EU funded critical infrastructure protection project
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SEE	South East Europe
SLTT	state, local tribal and territorial
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector-Specific Agencies
SSP	Sector Specific Plan
TSA	Transportation Security Administration
UK	United Kingdom
UN	United Nations
US	United States
USD	United States Dollar
USCG	US Coast Guard
WTO	World Trade Organization

List of tables and figures

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.

CHAPTER 2

CRITICAL INFRASTRUCTURE PROTECTION IN THE EUROPEAN UNION

CHAPTER 2

Critical Infrastructure Protection in the European Union[3]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Based on a *Cybersecurity Strategy of the European Union*, the *Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union* (further *NIS Directive*) was adopted. It was adopted on 6 July 2016 with the obligation to be implemented into national legislation of all Member States until 9 May 2018 (European Parliament and of the Council, 2016). The *NIS Directive* presents main piece of legislation of the *Cybersecurity Strategy of the European Union* and is extremely significant in its nature and application. Legal basis of the *NIS Directive* is in Article 114 – *Treaty on the Functioning of the European Union*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2.2. Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union

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

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

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

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

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

2.3. Co-operation activities within the European Union

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter conclusion

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

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

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

CHAPTER 3

CRITICAL INFRASTRUCTURE PROTECTION IN NATO

CHAPTER 3

Critical Infrastructure Protection in NATO

Toni Mileski, PhD
University of Ss. Cyril and Methodius - Skopje
Faculty of Philosophy, Institute of Security, Defense and Peace

The approach and contribution of NATO in the critical infrastructure protection is still a topic of numerous political debates and scientific analyses. Although the complex role of NATO after the break-up of the bipolar world is a major feature in the years to come, we can conclude that with its evolution, the discourses of its interest are evolving as well. It is evident that the attempts for politicization and securitization of energy supply, the involvement and role of NATO in the field of energy security and critical infrastructure protection open a wide array of NATO's role.

What should be mentioned straightaway, and at the same time profiles the structure and character of the Alliance in the post-Cold War period is the Communiqué of the Riga Summit where special emphasis is placed on the protection of energy infrastructure as part of energy security. In this respect, it is important to note that NATO owns and operates significant strategic assets, including 10 different 12.000 kilometer pipelines for transportation of aviation fuel, passing through 12 NATO countries and connecting storage depots, air bases, civil airports, gas stations, refineries and ports, including the largest NATO pipeline system, i.e. the Central European Pipeline System (CEPS). For four decades, NATO has been managing CEPS and pursuing its commercial and business interests, it is being rented for industrial purposes providing aviation fuel for major commercial airports in Europe. The entire aircraft fuel for the needs of the airlines at the Brussels airport, as well as most of the fuel for the airports in Frankfurt (Germany) and Schiphol (Netherlands) is acquired through CEPS. World War II memories were still very fresh when the construction of CEPS began and it was designed to withstand the toughest war conditions. It has numerous pumping stations, strengthened critical areas, entrenched pipelines and emergency response and repair teams are available at any time. In conditions of intensified dialogue between the Euro-Atlantic partners for energy security and its transport systems, NATO has a lot to offer. (Bell, 2009: 268).

In this Chapter, following these undisputed facts, we will try to tackle several important issues through a critical analysis of one segment of the involvement and the role of NATO in protecting critical infrastructure. One of them is whether NATO is doing excessive securitization and militarization of the energy sector, which is dominantly regarded as an exceptional economic issue, and whether there is an adequate role and opportunity for NATO's involvement in protecting critical infrastructure within strategic concepts, especially after the end of the Cold War.

3.1. Strategic Framework of Critical Infrastructure Protection Concept

In general, we can agree that NATO has been regulating and strictly protecting its critical infrastructures since its establishment. According to the Alliance's founding document, there are several possible scenarios in which NATO should play a role in critical infrastructure protection. First, to provide support to military operations of the Alliance under the provision of Article 5. Second, to provide support of crisis response operations beyond the provision of Article 5. Third, to provide support to national authorities in emergencies of non-military character. Fourth, to provide support to national authorities in protecting their population from the consequences of weapons of mass destruction. Fifth, to establish co-partnership with partners in the area of civil emergency planning. (Babos, 2016).

According to the protocol created during the Cold War, NATO provides security for critical infrastructure of the Alliance and its Member States. In order to provide a coordinated approach to civilian emergency planning, the key role is assigned to the Civil Emergency Planning Committee, which directly reports to the North Atlantic Council.

Civil emergency planning is an important activity in the prediction process and it is directed at coordinating national resources. In the context of natural and man-made disasters, the contracts strengthen NATO's role in emergencies. Examples may include the "NATO Policy on Disaster Assistance in Peace Time" of May 9, 1995 or the statement "Enhanced Practical Cooperation in the field of Disaster Relief" of May 29, 1998. In addition, NATO's 1999 Strategic Concept recognizes major catastrophes as a source of concern for security and stability.

The term "critical infrastructure protection" – according to Clinton's Directive from 1998, after the terrorist attack of September 11, 2001, was immediately placed on the agenda of the North Atlantic Council. After the September 11, 2001 attacks, the NATO Summit in Prague initiated the "Civil Emergency Planning Action Plan". In particular, Article 4, item d of the Declaration from the Summit states: "…we are committed, in cooperation with our partners, to fully implement the Civil Emergency Planning Action Plan for the improvement of civil preparedness against possible attacks against the civilian population with chemical, biological or radiological agents. We will enhance our ability to provide support, when requested, to help national authorities to deal with the consequences of terrorist attacks, including attacks with chemical, biological, radiological and nuclear weapons against critical infrastructure, as foreseen in the Civil Emergency Planning Action Plan". (Prague Summit Declaration, 2002). In addition, testing exercises and subsequent improvement of interoperability were planned. At the same time, the "Partnership Action Plan against Terrorism" was published.

After September 11, the readiness of NATO Member States in the area of critical infrastructure protection was considered. The result of such activity is the concept document for critical infrastructure protection, prepared by the Senior Civil Emergency Planning Committee. The main goals are summarized in the exchange of information among stakeholders, assistance and development of training and education programs that contribute to identifying critical infrastructure, determining research to support critical infrastructure protection and assistance

during exercise activities. Planning Boards and Committees of the Senior Civil Emergency Planning Committee have commenced the necessary studies. National experts from governments and industry, as well as military representatives, coordinate the planning of eight technical domains: civil aviation, civil protection, food safety, industrial production and logistics, internal land transport, issues in the field of medicine, shipment and in the end civilian electronic communications. In 2005, the Senior Civil Emergency Planning Committee adopted and adjusted the Action Plan in order to cover efforts during and after terrorist attacks with chemical, biological, radiological and nuclear weapons. The plan focused on critical infrastructure protection and victims support.

Consequently, the increased activity of European Allies in the field of critical infrastructure protection is the result of the terrorist attacks in Madrid in 2004, the cyber-attacks in Estonia in 2007, the Russia-Georgia conflict in 2008, the pirate attacks that have been continuously occurring since 2008 in the Gulf of Aden and the shores of Somalia as well as the escalation of the Russia-Ukraine relations. In addition to the conceptual and strategic document for critical infrastructure protection, NATO, today, also creates and implements policy and practices at operational level. (Babos, 2016: 12).

At strategic level, the beginnings of NATO's interest and activities in the area of critical infrastructure protection date back to 1990 and the NATO Summit held in London. As a result of the guidelines given at the London Summit, a new Strategic Concept of NATO was created in 1991. In this strategic document, the Alliance begins to promote critical infrastructure security related to vital energy resources. Namely, according to the NATO Strategic Concept of 1991, the disruption of the flow of vital resources is defined as a potential security threat to the interests of the Alliance (paragraph 12) (The Alliance's New Strategic Concept, 1991). At the Washington Summit in 1999, the very same conclusion was noted by the Alliance in the then approved new Strategic Concept (paragraph 24) (The Alliance's Strategic Concept, 1999).

According to the content of NATO's Strategic Concept adopted at the Lisbon Summit in 2010, critical infrastructure is first and foremost clearly and unambiguously mentioned in the section on "cyber" attacks. Paragraph 12 underlines that "cyber" attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure. In addition, it is emphasized that "cyber" attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.

Paragraph 19 of the Strategic Concept emphasizes the commitment to develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners and consultations among Allies on the basis of strategic assessments and contingency planning (Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, 2010: 11-17).

Strategic commitments to NATO's critical infrastructure grounded in its strategic concepts reflect the intense debates on energy security as an issue that is intensely debated internationally. NATO's activity in this field practically dates back even before it was included in the strategic concepts. Namely, during the Cold War, the Alliance maintained and provided a gas pipeline system for the supply of natural gas to own forces and the critical infrastructure in Europe.

It is this discourse that will serve us to explain in more detail the complex content about the place, the role and the involvement of NATO in critical infrastructure protection.

3.2. Involvement and Role of the Alliance in Critical Energy Infrastructure Protection

As previously mentioned, problems related to energy security, including critical infrastructure protection, have not been a basic thematic content exclusively to economic forums for quite some time. This means that these topics are increasingly becoming the main content within the framework of international political meetings at the highest level. Trade exchange of basic energy resources is not only an economic issue, but it is rather becoming a political issue as well. Moreover, given that NATO as a military-political Alliance more and more put regularity and stability in the energy supply on its work agendas, clearly it can be concluded that the supply of energy and everything related to that supply is a topic of the security discourse, but an interest of NATO as well.

However, NATO's involvement in critical infrastructure protection has its own critical component. We will try to analyze it through the corpus of issues related to energy security and critical energy infrastructure.

The possibility of involvement and the role of NATO in the field of energy security has two crucial moments. The first moment has a more military and security focus that reflects the dual need of the Alliance to implement practical and logistic planning for protection of energy supplies, especially oil, while maintaining wider security of its Member States and stability of own operational capability.

This conclusion implies consideration of the military threats to energy facilities as well as the routes for supplying energy resources. The possibilities for escalation of efforts to establish control over producers, transit countries in terms of energy (pipelines, gas pipelines) and their own security are the relevant factors of possible military confrontations. Some analysts argue that the possibility of accessing energy resources can become the subject of major military confrontations and poses a serious problem in the functioning of the modern international system. Pirate and terrorist attacks increase this risk.

According to a report by the United Nations, in the period from 2010 to 2014 the energy sector was extremely vulnerable to terrorist attacks. Most of the terrorist attacks in the given period occurred in Pakistan (439), then in Yemen (170), Colombia (161), Iraq (146), the Philippines (73), India (42), Nigeria (38), Thailand (37), Turkey (28) and the like (CTED Trends Reports, 2017: 4-5). Such wide geographical dispersion of terrorism and critical energy infrastructure phenomena enables

maritime energy security to have vital significance. This requires effective tackling of illegal activities and disruptions of energy supply to a relatively large operating space. It is known that more than two thirds of the world is covered with salt water and approximately 80% of world trade is waterway trade. What we can notice as an energy security problem is the fact that most of the world's oceans are not under state jurisdiction (Wilson, 2012).

The second moment for NATO's involvement in energy security discussions is more focused on political pressure and threats to energy security. This attitude can be identified and emphasized especially after the dispute between Ukraine and Russia's "Gazprom". A political pressure, which manifested itself with a stoppage of gas supplies, in early 2006. Russian authorities explained this act as solely due to economic reasons. The increase of oil and gas prices for the countries of the former Soviet Union marked the end of the era when they bought energy at a lower price. In this way, official Moscow seeks to keep the debate on the economic field, emphasizing that the price increase has economic and not political significance. Russia's finance and economy ministers stressed that the adjustment of Russian energy prices to world prices by 2011 is one of the conditions for Russia's admission to the World Trade Organization. Russia became a WTO member in 2012. (Radoman, 2007). Such events stimulated the discussion of energy security and critical infrastructure protection within NATO.

Both moments undoubtedly resulted in a conceptual difference in terms of achieving the main goal. Namely, the dilemma is set to the following level: should the Alliance adopt a broader "thematic" approach to energy security and critical energy infrastructure protection, in which the interests of the "producer", "transit" and "consumer" state are effectively seen in similar light – against threats that undermine everyone's interest, such as an attack on the main supply route? Or it needs to adopt a more regional and direct approach, in which the interests of the "producer" and the "consumer" differ – which basically carries the influence of a powerful Alliance in the support of the "consumer" country in what is considered a competitive "producer" – "consumer" dialogue.

NATO's practical action related to energy security dates back to July 30, 2007, when a fleet of six Alliance Members (Denmark, the United States, Germany, Portugal, Canada, and the Netherlands) headed for a long trip to Africa. The statement of former NATO Secretary-General Jaap de Hoop Scheffer, that the high priority of NATO Member States is maritime security and the provision of safe passages for the transport of fuels, determines the starting point for the Alliance's action in the context of energy security and route protection and critical energy infrastructure.

The main goal of NATO's mission was directed towards the Niger delta, where criminal gangs attacked oil installations and kidnapped workers who worked on oil platforms. For the first time in the history of NATO, joint maritime exercises were carried out along with the South African Navy, which in September 2007 also moved into dangerous waters off the coast of Somalia, where pirate attacks increased. The intention of this two-month mission was to demonstrate NATO's capabilities for the use of military assets and to guarantee the Law on the High

Seas, which, inter alia, includes the protection of the right for passage of the vital energy resources (Mileski, 2014: 47-48).

In the context of the need for the Alliance's involvement in energy security and critical energy infrastructure protection, the Riga Summit, held in November 2006, is particularly important. In autumn 2006, NATO made the final preparations for the missions, and at the Riga Summit the Allies were still quite divided on whether energy security was part of the Alliance's mission. In this role of NATO, several Member States recognized the interests of the European Union. However, after a year of persuasions, the then Secretary General succeeded in putting energy security on NATO's agenda. First, Scheffer managed to impose this issue at an informal meeting between NATO officials and foreign ministers of the Member States of the European Union. Then, in February 2006, at the Munich Conference on Security Policy, he reiterated the commitment to expand and deepen formal political and security discussions within NATO to cover more key issues, while undoubtedly referring to energy security. In order to continue further discussions, NATO leaders scheduled a NATO Forum on Energy Security in Prague, announcing the presence of a number of prime ministers, energy ministers, senior NATO officials, as well as senior representatives from the global energy community. (Bell, 2009: 261-262). After numerous remarks by several governments of the Allies, especially France, the Secretary-General was confronted with new problems including the ban for the members of NATO's International Headquarters to give presentations at that Conference. The then NATO statement stressed that NATO had no formal role in the field of energy security and safety of oil and gas pipelines, and that NATO did not consider any military involvement in protecting oil and gas infrastructure in the Caucasus or any other region. However, until the NATO Summit in Riga, the US efforts as well as Europe's concern for Russia's use of gas and oil as an instrument for political influence, made it clear that NATO could no longer ignore energy security. In a document adopted at the Summit entitled "Comprehensive Political Leadership", NATO leaders point out that the violation of normal movement of vital resources will constitute one of the main threats to the Alliance over the next 10 to 15 years. Recognizing the efforts of the NATO Secretary General, a consensus was reached, and implemented in the NATO Summit Declaration in Riga.

The Riga Declaration represents a significant starting point for any analysis of NATO's role in energy security and critical energy infrastructure protection. Namely, Article 45 of the Declaration stipulates that NATO's security interests can be affected by the disruption of the flow of vital resources. The Alliance supports a coordinated, international effort to assess risks to energy infrastructures and to promote energy infrastructure security. The individual engagement of NATO Member States has been identified even before the discussion on the role of the Alliance in the field of energy security. We can detect it in the period of the 1980-1988 Iran-Iraq war. Then, Britain, France and the Netherlands participated in "Earnest Will" Operation, providing the routes for tankers in the Persian Gulf (Varwick, 2008: 39).

After the Riga Summit, serious political disagreements between the Allies regarding NATO's role in the field of energy security remained evident. At the meetings of various political-military bodies, there have been more questions than answers. In February 2007, a Working Group on Energy Security was formed within

NATO for the first time. Its task was to point out all the issues that the Alliance had to answer before building any framework or policy on energy security, namely:

- define the role of NATO forces in the protection of energy infrastructure;
- identify problems in all NATO missions in providing safe transit corridors for oil and gas through the Strait of Hormuz and other specific locations, as well as providing a not provocatively presence at sensitive locations for oil and gas production;
- integrate polices for security of supply among all Alliance members (Mileski, 2014: 50).

Namely, the Riga Summit Declaration included a short paragraph explicitly announcing (for the first time) that energy security is a concern of NATO, giving the Alliance a task to explore the specifics of that role. In the Declaration, the nature of the discussion changed, so it is no longer about whether the Alliance has a role, that is, it confirms that it has one. The question is now about the nature of that role. Another important moment is the speech of the US Senator Richard Lugar on the side-lines of the Riga Summit. The speech points to the threats from terrorism, as well as to the fact that energy is likely to be a source of armed conflicts on the European scene as well as in the surrounding regions. In that way, Lugar emphasizes that it would be irresponsible for NATO to reduce its engagement in the field of energy security. However, his focus was directed to the potential of political manipulation of resources and the use of "energy weapons". Lugar's speech was the subject of attention of the entire international public.

After the adoption of the Riga Declaration, the political moment continued to gain greater significance, especially after the dispute over the discontinuation of gas supplies between Russia and Belarus in December 2006 and January 2007. The same thing happened in the years to come. On January 31, 2008, Russia halted gas supplies to Ukraine, due to unpaid bills and the price of gas. The Russia-Ukraine dispute over the gas price left ten countries from Central and Eastern Europe without that fuel. Countries like Moldova, Slovakia, Bulgaria, Serbia, Croatia, and North Macedonia remained without heating gas and electricity production**,** while Turkey, Greece, the Czech Republic, Poland, Hungary and Austria faced gas shortage. The political moment apparently had its peak in January 2009. The disruption of Russian gas supplies to Ukraine has caused major discomfort in the European Union because 40% of natural gas for the European Union is provided by Russia, and 80% of that gas flows through Ukraine. The crisis ended on January 19, following negotiations between the then Prime Minister of Russia, Vladimir Putin and the then Prime Minister of Ukraine Julia Timoshenko. It was agreed that in 2009 Ukraine would pay 20% lower price for the Russian gas than its market value, and from 2010 would pay the same price as other European countries, i.e. 470 USD per 1000 cubic meters. Until then, Ukraine had a preferential price for Russian gas of 179,5 USD per 1000 cubic meters (Mileski, 2014: 51).

Generally speaking, before the Riga Summit, the Alliance pointed to the issue of energy security rather unclearly, that is, NATO's activities were aimed at preventing the disruption of the flow of vital resources. Defining the disruption is the key challenge for the Alliance illustrating the gap in the consensus between

military threats to vital resources and those politically motivated. NATO's mandate defined in the Riga Declaration provides some clarification of the interests of the Alliance and their focus on security of energy infrastructure but not on other dimensions of energy security. The focused and limited agenda defined by the Riga Declaration set the stage for official talks in 2007 and early 2008. The then NATO Secretary-General Jaap de Hoop Scheffer, reiterated that the Alliance considered energy security a "collective" challenge for which "collective" response had to be ensured. A response, which would be broadly in line with coordination between national governments and international organizations. Furthermore, NATO's role in such a collective response would be focused where it could contribute, that is, the Alliance should consider its own role in protecting delivery routes, especially in case of transport of liquefied natural gas with offshore vessels and critical energy infrastructure protection when there is a certain high level of threat.

At the Bucharest Summit in April 2008, the same approach was confirmed. The Alliance will endeavour to contribute and fully coordinate with the activities of the international community, which contain numerous organizations that specialize in the field of energy security. Although there are still some obscure phrases – the Alliance will engage in "projecting stability" and promote international and regional cooperation. Moreover, the focus on civil defence and crisis management and energy infrastructure remains clear. This leads us to consideration of the "deepened" role that NATO could realize.

In this context, NATO's role could be geared towards contributing to coordinated international efforts to improve energy security in two broad areas: information sharing and planning, and response.

Firstly, information sharing is one of the key principles of energy security. NATO can contribute by acting as an important bridge between the energy and security community. This is clearly indicated by the Riga Declaration, and confirmed by the Bucharest Declaration, that is, NATO can contribute to the exchange of information acting as a forum for exchange of notifications. Certain considerations are moving in the direction of strengthening the link between the security and energy community through the creation of permanent monitoring and evaluation of the action mechanisms in cooperation with the International Energy Agency (IEA) and similar organizations, including companies. In addition, NATO can contribute to the exchange of data through the practical use of its assets and capacities. That is, marine surveillance and early warning assets can be used to provide immediate information on major maritime transport routes that are not sufficiently covered by the national capacities of certain countries. Secondly, the Alliance can contribute to the achievement of energy security by making available its own military capabilities and expertise where needed. Primarily it is referred to physical protection, patrolling and escorting the critical infrastructure pathways. NATO already has a clearly defined role in protecting oil and gas facilities in the North Sea in case of armed attacks. NATO's (and the EU's) naval capacities are already used to protect shipments of oil and gas in the Horn of Africa and West Africa region, especially from pirate attacks and terrorist attacks. Such threat response capabilities were manifested by operation Steadfast Jaguar 06, held in Cape Verde in June 2006.

Energy security has an appropriate position in NATO's new Strategic Concept of 2010, adopted at the NATO Summit held in Lisbon. As a continuation of the above mentioned paragraphs, in the part of the strategic framework that positions the concept for critical infrastructure protection of NATO, in Article 13 of the basic principles and principles of the new Strategic Concept of NATO, it is emphasized that all countries increasingly rely on vital communications, transport and transit routes dependent on international trade, energy security and prosperity. This implies greater international efforts to ensure their resistance to attacks or interruptions. Certain NATO Member States will increasingly become dependent on external energy suppliers, while in certain cases by external energy suppliers and distribution networks for their own needs. On a global level, the energy supply will face increased exposure to disruption in distribution. (Strategic Concept for the Defence and Security of the Members of the NATO)

These commitments represent the continuity of NATO's attitudes set forth in the Strategic Concept adopted in 1999. It is evident that it forms the basis for all further decision-making processes by the Alliance, and everything related to energy security. Paragraph 24 of this Strategic Concept enacted on NATO's 50th anniversary in Washington, states: "Any armed attack on the territory of the Allies, from whatever direction, would be covered by Articles 5 and 6 of the Washington Treaty. However, Alliance security must also take account of the global context. Alliance security interests can be affected by other risks of a wider nature, including acts of terrorism, sabotage and organised crime, and by the disruption of the flow of vital resources. The uncontrolled movement of large numbers of people, particularly as a consequence of armed conflicts, can also pose problems for security and stability affecting the Alliance. Arrangements exist within the Alliance for consultation among the Allies under Article 4 of the Washington Treaty and, where appropriate, co-ordination of their efforts including their responses to risks of this kind".

So, NATO Member States agree with consensus that terrorist attacks could be the basis for invoking the collective security guarantees contained in Article 5 of the NATO Treaty. Up to 1999, the Clinton Administration dealt with the bombings of US embassies and military forces abroad by Al-Qaeda, and urged the Allies to agree on extending the traditional concept and the reason for activating Article 5. Two years later, with the September 11, 2001 attacks, following the horrific scenes of the terrorist attacks on Twin Towers, a North-Atlantic Council statement followed, stating that the Council agreed that if determined that this attack against the United States was conducted from abroad, it would result in the activation of Article 5 of the Washington Treaty, stating that an armed attack against one of the Allies in Europe or North America will be considered an attack against them all. The collective self-defence effort embodied in the Washington Treaty for the first time faced situations different from those that existed before, but it still remains no less valid and essential.

What should be noted is that Paragraph 24 of the Strategic Concept does not end and does not cover only the "terrorist act". Furthermore, violations of the course of vital resources constitute an additional basis for invoking Article 4 and even a coordinated response (if necessary) through collective security in accordance with

Article 5. This does not mean that there is an automatic response mechanism if such situations arise. The existence of this paragraph does not mean that any oil crisis will result in invoking Article 5 by NATO. This will depend above all on the nature of the circumstances, the success / failure of diplomatic measures, but also the ability to reach consensus within NATO.

Regarding the Lisbon Declaration, the content in the field of energy security is highlighted in Article 41. Namely, the Article points out that the stable and secure energy supply, diversification of routes, suppliers and energy resources, as well as the connection to energy networks, remains to be of critical importance. The Alliance will continue consultations on the most immediate risks in the field of energy security in line with the decisions taken at previous summits and in line with the new Strategic Concept from Lisbon. The Alliance will further develop capacities to contribute to energy security, concentrating on the areas discussed at the Bucharest Summit. In advancing the work of the Alliance, cooperation and consultations with partners and other international actors will be strengthened in order to integrate energy security considerations in NATO policies and activities. It will be requested to prepare an interim report on the progress achieved in the area of energy security for the Foreign Ministers' meeting in December 2011, and a further report for consideration at the forthcoming NATO Summit (Lisbon Summit Declaration, 2010).

At the Chicago Summit, the continuity of interest in energy security remains. In a Declaration emerging from the Chicago Summit, Article 52 states, same as the previous Summit in Lisbon, that a stable and reliable energy supply, diversification of routes, suppliers and energy resources, and the interconnectivity of energy networks, remain of critical importance. While these issues are primarily the responsibility of national governments and other international organisations concerned, NATO closely follows relevant developments in energy security. At the Chicago Summit, NATO noted a progress report, which outlines the concrete steps taken since the last Summit of the Alliance and describes the way forward to integrate, as appropriate, energy security considerations in NATO's policies and activities. NATO will continue to consult on energy security and further develop the capacity to contribute to energy security, concentrating on areas where NATO can add value. To this end, it is noted that for the aforementioned goals, the Alliance will work towards significantly improving the energy efficiency of own military forces; develop own competence in supporting the protection of critical energy infrastructure; and further develop own outreach activities in consultation with partners, on a case-by-case basis. On this occasion, the Alliance welcomes the offer to establish a NATO-accredited Energy Security Centre of Excellence in Lithuania, as a contribution to NATO's efforts in this area. The Council's task is to continue to refine NATO's role in energy security in accordance with the principles and the guidelines agreed at the Bucharest Summit and the direction provided by the new Strategic Concept as well as the Lisbon decisions. The Council is tasked to produce a further progress report for the next NATO Summit (Chicago Summit Declaration, 2012).

At the NATO Summit held in Cardiff, Wales in 2014, the final declaration of the Summit in Article 109 mentions the following: For NATO of critical importance and

permanent commitment are constant and reliable energy supply, the diversification of routes, suppliers and energy resources, as well as the interconnectivity of energy networks. While these issues are primarily the responsibility of national governments and other international organizations, NATO closely follows relevant developments in the field of energy security, including in relation to the Russia-Ukraine crisis and the growing instability in the Middle East and North Africa region. NATO will continue to consult on and further develop its own capacity to contribute to energy security, concentrating on areas where NATO can add value. In particular, the awareness of energy developments with security implications for Allies and the Alliance is especially emphasized; further develop NATO's competence in supporting the protection of critical energy infrastructure; and engagement in improving the energy efficiency of military forces, with the Green Defence Framework highlighted (Wales Summit Declaration, 2014).

The Green Defence Framework is a significant step forward that was made at the Cardiff Summit. In short, this Framework provides the basis for increased knowledge sharing and coordination of research that can support the development of cheaper and more efficient green solutions for defense capabilities and deal with a range of modern and emerging security challenges such as energy security, global climate change, defense expenditure and logistic challenges to gaining energy on the battlefield (Larsen, 2015).

In 2016, the host of the NATO Summit was Poland, that is, Warsaw. The final declaration of the Summit in Article 135 emphasises that energy development and movement can have significant political and security implications for the Alliance, as demonstrated by the crises to NATO's east and south. It is concluded that a stable and reliable energy supply, the diversification of import routes, suppliers and energy resources, as well as the interconnectivity of energy networks are of critical importance for NATO. Reaching these commitments will allow for increased resilience against political and economic pressure. While these issues are primarily the responsibility of national governments and other international organisations, NATO closely follows the security implications of relevant energy developments and attaches particular importance to diversification of energy supply in the Euro-Atlantic region. For these reasons, it is underlined that NATO will continue to further enhance its own strategic awareness in this regard, including through sharing intelligence and through expanding own links with other international organisations such as the International Energy Agency and the EU. In doing so, it will be of particular importance to consult and share information on energy security issues of particular concern to Allies and the Alliance, with a view to providing a comprehensive picture of the evolving energy landscape, concentrating on areas where NATO can add value. NATO will also continue to develop its own capacity through energy security considerations in training, exercises, and advance planning. The main objective is to support national authorities in protecting critical infrastructure, as well as enhancing their resilience against energy supply disruptions that could affect national and collective defence, including hybrid and cyber threats. NATO's commitment will be to further improve the energy efficiency of military forces through establishing common standards, reducing dependence on fossil fuels, and demonstrating energy-efficient solutions for the military.

A progress report on NATO's role in energy security was noted at the Warsaw Summit (Warsaw Summit Communiqué, 2016).

At the last NATO Summit held in Brussels in 2018, the official final declaration states that energy security plays an important role in common security. At the same time, the allegations from the previous summit are reiterated that a stable and reliable energy supply, the diversification of routes, suppliers and energy resources, as well as the interconnectivity of energy networks are crucial and increase the Alliance's resilience against political and economic pressure. While these issues are primarily the responsibility of national authorities, energy development can have significant political and security implications for the Allies, and will also affect NATO partners. As a result, NATO will continue with regular consultations with the Allies on issues related to energy security. It is especially emphasized that it is essential to ensure that members of the Alliance are not vulnerable to political or forced manipulation with energy, which is a potential threat. Therefore, the Allies will continue to seek diversification of their energy reserves, in accordance with their needs and conditions. NATO will mitigate its own role in energy security in accordance with established principles and guidelines and will continue to develop NATO capacity to support national authorities in protecting critical infrastructure, including against malicious hybrid and cyber activities. NATO will continue to further enhance its own strategic awareness, through sharing intelligence and expanding own links with relevant international organisations such as the International Energy Agency, International Renewable Energy Agency and the EU, as appropriate. NATO will also improve the energy efficiency of military forces, through the use of sustainable energy sources, when appropriate. These assertions indicate that between the two NATO Summits in Warsaw and Brussels the directions of NATO's action in the area of energy security and critical infrastructure protection have not changed (Brussels Summit Declaration, 2018).

The continuing interest of the Alliance for the protection of critical (energy) infrastructure is a constant that can be recognized from the guidelines that emerge from the Summits' final Declarations. From them, it is clear that preparation of reports by the North Atlantic Council for the advancement of the Alliance in the field of critical infrastructure protection and energy security is required.

3.3. Critical Review of the Complex Role of the Alliance

According to the foregoing, NATO is mandated to re-examine its potential role in the field of energy security, internationally. The Riga Declaration, in particular the section on energy security, faces a series of complex elements that slow down the practical definition of the role of the Alliance. Officials and analysts from most NATO Member States are of the opinion that energy security remains a national problem, and that it should be treated as such. Therefore, according to them, deployment of NATO troops on oil platforms or safeguarding oil pipelines and gas pipelines is unthinkable scenario. In this context, a NATO diplomat responding to speculation about the deployment of troops as "pipeline police" in regions such as the Caucasus, will emphasize that energy security and safety of installations and transport routes constitute a national responsibility. The engagement of the

Alliance should primarily focus on giving advice and assistance rather that actively engaging on the field. (Mileski, 2014: 56).

Turkish experts and analyst's express similar views pointing out that by fighting against the Kurds, the Turkish state made much more than the Alliance in terms of protecting critical energy infrastructure. Also, Azerbaijan, where a significant energy route passes (Baku-Tbilisi-Ceyhan Pipeline) via former Deputy Prime Minister Abid Sharifov emphasizes that the Alliance has no experience in protecting pipelines and communications that pass through non-NATO countries. Such views on the lack of need for assistance by NATO, specifically for the indicated oil pipeline, arise from the fact it is protected by both the Azerbaijani government and companies that believe that protection has been achieved through other measures such as: deep digging of oil pipelines and the indication of the locals for the importance of the pipelines safety.

On the other hand, if we move to the north, more precisely the North Atlantic region, and analyze the discussions of their experts and analysts we will see different standpoints. Namely, the Norwegian Sea and the transport routes of oil and natural gas that pass through here, promote discussions on the need to consider maritime safety issues. It is underlined that NATO Members from both sides of the Atlantic must work together on energy security, as a central part of the Alliance's security policy, primarily on transport security and then on energy security. According to Bjorn Bjarnarssonar, energy security poses a new dimension that redefines the northern areas of the Atlantic region of NATO's political and military scene, that is, reaffirms NATO's maritime identity.

According to other opinions, the energy security role would divert or violate the NATO agenda to the detriment of existing missions. Energy security is also linked to other issues of the complex NATO agenda, such as the debate on further extension of Article 5 including energy security. In his speech on the side-lines of the Summit in Riga, already mentioned Senator Lugar suggested effective energy strategies to include new relations with the countries of the Caucasus and Central Asia, and in particular the relations with Kazakhstan and Azerbaijan, where possible NATO membership must be put on the table (Mileski, 2014: 59).

Arguments for the extension of Article 5 concern the possibility of destroying national economies if energy is used as a "weapon". In this way, the Alliance would commit itself to an appropriate response to the attempts and use of energy as a "weapon" against its Member States.

Although cooperation with other international organizations is an important intention noted in Riga, Lisbon, Chicago, Cardiff, Warsaw and Brussels, it is also proving to be quite problematic. Defining NATO's role within energy security allows wider discussion and presentation of different opinions that are often at the same "frequency". This can be illustrated, for example, with the difference in defining the threats to energy security at national and institutional level. Taking into account the different geographical regions, resources and infrastructure capacities, and therefore their individual energy strategies, most countries in the EU and NATO see a different way of the energy situation. Accordingly, within each organization, there is a problem of defining any advanced degree of clarification and consensus on the nature of the threat and to whom it relates.

A growing number of EU and NATO Member States regard the energy crisis as an economic problem that should be primarily regulated on the market, rather than by external political and security measures. Generally, we could agree that the United States is striving to accept energy security as a protection of energy supplies, while the EU defines it in terms of managing energy demand. These different starting points in the definition of energy issues pose an additional complicated situation, especially after the various reactions within the EU and NATO on some of the issues that brought energy security to the agenda of the Alliance. All this undermines the prospect of establishing complementary energy relations between NATO and the EU.

An additional problem is the Russian view of the discussions on the inclusion of energy security on the NATO agenda. The Alliance is striving the debate on energy security not to be interpreted by Moscow as an anti-Russian signal. In this regard, the statement of the Russian Foreign Minister at the end of 2007, Sergey Lavrov, is especially interesting. Namely, he condemned the politicization of energy security to the detriment of the producer countries and stressed that what is purely economic is politicized by an attempt to unite consumers to confront the Russian energy monopoly (Monaghan, 2008). As NATO begins to discuss energy as a security issue, Moscow is also doing the same, compiling a new military doctrine in which energy security has its place. In particular, in the new military doctrine of Russia from 2014, in the part of carrying out the main tasks of building and developing the armed forces and other troops and organs, among other things, they are achieved by establishing territorial troops for protection and defense of military, governmental and special facilities, that provide vital functions of the population, operation of transport, energy facilities, as well as objects that pose an increased danger to the life and health of people (Military Doctrine of the Russian Federation, 2014).

In the process of redefining NATO as a security guarantor for its Members, the need for a serious consideration of the energy supplies safety is increasingly required. The threats to energy security are widely established in international politics, but also at the national level. In addition, the problem is seriously elaborated in the academic community as well. However, the positions that are not related to the acceptance of NATO's role in resolving threats to energy security are still dominant.

As for the existing grounds of the Alliance, regarding Article 5, we can see that energy security is somehow contained in it. Article 4 of the Washington Treaty stipulates that the Parties "will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened". Article 5 is also potentially relevant, taking into account the nature of most threats "the Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them" (The North Atlantic Treaty). Taking into account the fact that this does not distance the energy plants from other targets, and on the other hand the nature of the threats to energy infrastructure by terrorists, pirates and even countries, most likely will take the form of armed attacks, we can assume that an armed attack on an energy plant may be the reason for invoking Article 5. The only exception

would be the deliberate termination of production of the necessary quantities of fuels and their delivery to the end consumers, which would influence national economies and would have taken certain political positions the country of origin. In this case, the reference to Article 5 would be indicative.

Negative connotations regarding the proposed agenda for NATO's role in energy security seem to be understood too simplified. That is, speculations generally go in the direction solely of military response of the Alliance in case of endangering energy security. If this is followed up by the unrealistic agenda or the provocation for discussion on changing the existing Article 5 of the Washington Treaty and the potential membership of Kazakhstan and Azerbaijan, a new strategic horizon is evident which can shape the future international context in which the Alliance will function.

In defining its own role within energy security, the Alliance faces two parallel debates aimed at defining the disruption of energy supply. Will it be a military disruption, caused by armed attacks or perhaps in the context of a competition for access to certain resources? It should determine the efforts of the Alliance in order to find the most appropriate solutions. That is, its engagement would work in the direction of cooperation with partners, capacity building, defense reform and training of partner countries. In extreme cases, it may be possible to include military infrastructure protection against armed attacks. The second debate is aimed at determining the disruption of energy supply due to political reasons for such an act, which are often difficult to define and prove. In this case, it is very difficult to count on the consensus of all partners in eventual undertaking of certain measures. On the other hand, such a situation can motivate consideration of certain solutions within the Alliance, which might be the intention to improve its own efficiency in energy consumption as a means of reducing dependence on external conditions.

However, the Alliance will have to work more actively on its own role in energy security, in the context of its evolving path of survival and functioning on the international security scene. One of these directions seems to have established itself with the establishment of the NATO accredited Energy Security Centre of Excellence in Lithuania. This act clearly shows that energy security debates from theoretical elaborations, slowly but surely, result in practical actions on the ground. Namely, the Centre started functioning in 2012 as an international military organization under NATO's mentorship. With this act, the role of NATO in the field of energy security is more clearly determined. The concept for this Centre is in line with the set strategy for the so-called NATO's "smart defense", established at the Lisbon Summit. The Centre will work in the field of technical, scientific and academic research that should contribute to the appropriate assessments and analyses of the contingency risks. The Centre should also contribute through appropriate recommendations and suggestions for effective and cost-effective solutions to operational energy problems in support of military requirements. The Centre should support the research of alternative energy resources and the development of environmentally friendly and efficient military capabilities. Furthermore, it should facilitate engagement in education and exercises, as well as provide scientific, technical and academic analyses from various aspects of energy supply and critical energy infrastructure (NATO ENSEC COE).

We will specify several examples on how the Alliance should be set in case of potential energy crises. According to certain scenarios that are hypothetical, but not impossible, a NATO Member State may request additional consultations in accordance with Article 4, and as a result of endangering the security of energy supply. For example, in January 2006, Bulgaria (a NATO member since 2002) rejected Gazprom's request to re-examine the price it should pay for natural gas. If Gazprom cut off the natural gas supply to Bulgaria (as it happened with Ukraine, Moldova and Georgia), the question arises as to whether Bulgaria would seek additional consultations under Article 4. The only way to find out the answer to such a question is to bring it out within NATO. In addition, Bulgaria is not the only NATO member with very high dependence on imported oil or natural gas. What is more, Slovakia 100% dependency, the Baltic States with 100% dependency, Poland with 99% dependency, Bulgaria with 94% dependency, Czech Republic with 82% dependency and Hungary with 81% dependency are in a similar situation (Bell, 2009: 266).

Ukraine is not a NATO member, at least not until today. On NATO's 60th anniversary in 2009, Poland and the United States strongly urged its accession to the Alliance. However, regardless the timeframe about favouring Ukrainian membership in NATO, it is difficult to imagine how NATO Allies will adhere to the Alliance's Strategic Concept, if, after the eventual Ukrainian membership, Russia decides to stop the supply of gas again. Similar concerns exist for Georgia (which also aspires to join NATO). A recent military conflict between Georgia and Russia in August 2008 underscored the risk of including former Russian Allies (who play a key role in energy security) in the Alliance. If Georgia were a NATO member, Russia's 2008 assault would put the Alliance under pressure to fulfil its military commitments. Emphasis is placed on Iran and the current nuclear crisis that is taking place there.

The European Union and the United States have stressed that they will never allow Iran to acquire nuclear weapons. Speculation about a possible preventive war aimed at Iran's nuclear facilities is becoming increasingly louder. However, at the same time, measures have been taken by the UN Security Council, but also by the United States and the European Union, mainly expressed through economic sanctions, which seek to force Iran to finally stop its nuclear program. However, the Iranian Government made it clear that any more rigorous measures towards Iran adopted by the UN Security Council would result in a reduction or total stoppage of Iranian oil exports to Western countries. Any obstruction of the transit of oil through the Ormut Strait will result in catastrophic consequences for many world economies. The events on the Arctic will also be interesting. Due to global warming, the vast oil and gas resources in that part of the world will finally become available (it is assumed that the Arctic possesses 25% of the total oil and gas reserves), and even 4 NATO Member States (the USA, Norway, Denmark and Canada), but Russia as well, will be direct participants as well as competitors for access to these resources. So, in conditions of incomplete defining of NATO's position on energy security, the only way to find out what is going to happen in the future is to go with the flow on the events that are ahead of us, and the answers will come by themselves. After the attacks on Iraq by the Allies, it became clear that

NATO would play the key role in dialogue for strategic and political consultations and coordination between the Allies from Europe and North America. In the future, it is assumed that this partnership will be strengthened, and dialogue will be further intensified, as well as the need for political and security consultations and coordination at the highest level in the Alliance, as there will be few issues that will be more important than energy security. The most likely source of armed conflicts in the European area and the surrounding regions in the future will be the lack of fuels and manipulation with them. Therefore, it is logical to assume that NATO Member States will be increasingly engaged in missions that are directly or indirectly related to energy security. If the Alliance wants to preserve its role and continue to be relevant to the development of global security in the mid-21st century, it will have to clarify its position and continue its coordination with other governmental and non-governmental organizations towards the realization of a common and a comprehensive transatlantic energy security policy. In other words, NATO should also use its status as an intergovernmental organization, but also its comparative advantage over other international organizations and that is its military capability.

Chapter conclusion

Analyzing NATO's Strategic Concepts, we can immediately assume that the Alliance regulates and protects its critical infrastructure. A wide range of opportunities and scenarios for NATO's involvement in protecting critical infrastructure gives the impression that at some points the militaristic approach is far beyond the Alliance's strategic commitments. However, the dilemmas that have been analyzed, related to the field of energy security and energy critical infrastructure, do not yet give a precise answer whether the energy sphere is purely an economic issue and whether energy issues can solely be regulated with military force. In this regard, NATO's emphasis should be placed on the support of national authorities, their strengthening and support for the successful and effective protection of critical infrastructure. The debate over the change of Article 5 and the explanation for the collective security of the Member States is more a form of strengthening the efforts to involve the Alliance in operational actions for concrete involvement in practice.

Analyzes by relevant authorities say the main responsibility for energy security issues should be left to the European Union, and NATO should stay aside. The European Union has a key role that it can and must play. This primarily concerns the activation of the necessary diplomatic measures towards Russia and the maximization of efforts to ensure Russian ratification of the Energy Charter and its transport protocols. In addition, intensification of efforts to define energy security within the European Union is needed, as well as new initiatives aimed at creating a single European energy market, resolving market disruptions, encouraging diversification and developing new technologies, and initiating programs to protect the European critical infrastructure. The European Union can and must expand its dialogue and cooperation with the United States in the field of energy security. Nevertheless, Norway and Turkey (still) are not members of the European Union,

which means that at the meetings of EU ministers, no one officially represents the North Sea oil supply, nor the possibility of reducing European dependence on Russian oil and gas represented by the realization of the Baku-Tbilisi-Ceyhan pipeline (Bell, 2009: 267).

The EU-US dialogue does not include Canada, leaving another country with huge resources away from these processes. However, these three countries (Norway, Canada and Turkey) are members of NATO and they exist as equal partners within. So, coordination between NATO and the European Union will be a winning combination for both sides. If anything, the dialogue (both at the informal level and in the regular meetings between the North Atlantic Council and the European Union Political Security Committee) is inevitable on issues related to the protection of critical infrastructure. Dialogue can be accomplished in many other places, especially within the OSCE, but also in the G-8 (Russia was chair in 2007, and the then President Putin imposed energy security as a key topic for discussion). The NATO-Russia Council is another place where political dialogue on these issues can be realized. The Council is not intended exclusively for talks for which there is agreement between the two Parties. It is also a place where all the issues with deep disagreements are expressed, and all the views of the Euro-Atlantic Allies about Russian energy use as an instrument of foreign policy should be presented here.

CHAPTER 4

CRITICAL INFRASTRUCTURE PROTECTION IN THE UNITED STATES

CHAPTER 4

Critical Infrastructure Protection in the United States

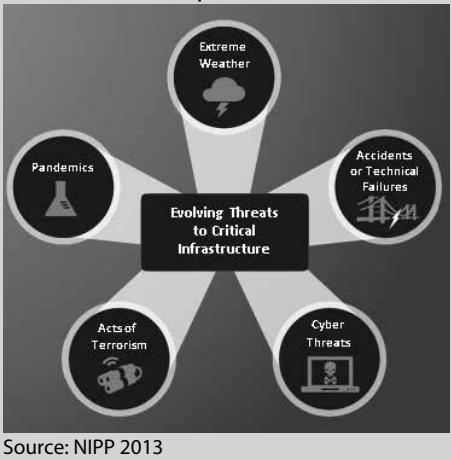
Matthew Vatter, MSS, MSST
US Army Colonel (Retired)
Assistant Commissioner for Enforcement, Minnesota Department of Commerce
Richard J (Rick) Larkin, MA, CEM
Emergency Management Practitioner
Minnesota, USA

4.1. The Organizational Structure of Critical Infrastructure in the United States

In practical terms, critical infrastructure is the power we use in our homes and businesses, the water we drink, the transportation we use to move people and commodities. It is the roads and bridges across the country, the malls in which we shop and the sporting venues we visit. It is our communication systems and our banking and finance systems. All in all it is the structure that enables everyday life as we have come to know it in the United States.

The United States identifies 16 Critical Infrastructure sectors. The systems and assets in these sectors are vital to the general structure and operations of national economy, public health and safety and the overall safety and security of American citizens. Presidential Policy Directive 21 (PPD-21) outlines the policy ensures a strong, resilient and secure system for protecting American critical infrastructure (The White House, 2013). Presidential Policy Directive 7 (PPD-7) established a national policy for federal departments and agencies to identify and prioritize critical infrastructure (Department of Homeland Security, 2003). Having federal level guidelines to direct efforts of federal agencies establishes roles and responsibilities across government and creates the foundation upon which protection activities occur.

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



Source: NIPP 2013

Separating critical infrastructure into 16 sectors facilitates the assignment of sectoral responsibilities within government and to private industry stakeholders. Sector-Specific Agencies (SSA) are identified to provide a lead resource for the

organization of multi-agency and stakeholder efforts to secure key sector assets. SSAs in coordination with the Secretary of Homeland Security prioritize critical infrastructure based on threat and vulnerability analysis, collaborate with sector specific critical infrastructure owners and operators, carry out incident management, provide technical support and assistance and help mitigate incidents. SSAs are also responsible for regular reporting to the Department of Homeland Security the overall state of preparedness within their assigned sectors and to identify areas of concern. SSA are charged with considering Critical Infrastructure Protection from and "All-Hazards" approach. The Term "all-hazards" means that incidents and threats considered come from natural and human-caused sources and apply to life, property, the environment and public health and safety. All-hazards includes natural disasters, industrial accidents, acts of terror, pandemics, cyber incidents, sabotage, and destructive criminal activities that target critical infrastructure (Department of Homeland Security, 2019).

The table identifies the 16 Critical Infrastructure sectors and the Sector Specific Agencies for each sector as well as a brief description of the areas of responsibility for each sector.

Table 2:
US Critical Infrastructure Sectors and Sector Specific Agencies

Sector and Specific Agent	Description
Chemical: Department of Homeland Security	The chemical sector is responsible for the manufacture, storage, use and transport of potentially dangerous chemicals relied upon by a wide array of other critical infrastructure sectors.
Commercial Facilities: Department of Homeland Security	The commercial facilities sector includes sites that draw large groups of people for lodging, business, entertainment and shopping. These facilities are characterized by having open access to the general public with a vast majority being privately owned.
Communications: Department of Homeland Security	The communications sector provides an enabling function across all sectors of critical infrastructure. It includes terrestrial, satellite and wireless communications.

Critical Manufacturing: Department of Homeland Security	The critical manufacturing sector includes those manufacturing capabilities that underpin many portions of other critical infrastructure sectors. They include primary metals manufacturing, machinery manufacturing, electrical equipment, appliance and component manufacturing and transportation manufacturing.
Dams: Department of Homeland Security	The dams sector provides critical water retention and control which includes hydroelectric power generation, agricultural irrigation, sediment and flood control, river navigation and industrial waste management.
Defense Industrial Base: Department of Defense	The defense industrial base sector is comprised of domestic and foreign companies that provide the materiel and services necessary to build, maintain, mobilize, deploy and sustain US military operations.
Emergency Services: Department of Homeland Security	The emergency services sector provides day to day as well as emergency response and recovery services. It is organized primarily at the federal, state, local tribal and territorial levels of government and includes police, fire, and emergency medical services organizations capable of all-hazard response.
Energy: Department of Energy	The energy sector describes the infrastructure that provides energy resources underpinning all sectors of critical infrastructure. 80 percent of the country's energy infrastructure is privately owned.
Financial Services: Department of Treasury	The financial services sector includes depository institutions, investment institutions, insurance companies and other credit and financing organizations that enable the transfer of financial products and services.

Food and Agriculture: US Department of Agriculture and Department of Health and Human Services	The food and agriculture sector provides for the production, manufacturing, and storage of the nations food and agricultural products supply.
Government Facilities: Department of Homeland Security and General Services Administration	The government facilities sector oversees buildings located in the US and overseas owned or leased by the US government that house embassies, military installations, courthouses, national laboratories, critical equipment and systems.
Healthcare and Public Health: Department of Health and Human Services	The healthcare and public health sector protects all sectors from terrorism, infectious disease and natural disasters. It is responsible for prevention, resiliency response and recovery to public health related issues.
Information Technology: Department of Homeland Security	The information technology sector encompasses the people, hardware and software necessary for the function of government, academia, private sector businesses and the general public. In coordination with the communications sector, is responsible for the internet.
Nuclear Reactors, Materials and Waste: Department of Homeland Security	The nuclear reactors, materials and waste sector includes nuclear power generation, medical isotopes and nuclear and radiological research. It also oversees the movement of radiologic cargo in coordination with the transportation sector.
Transportation Systems: Department of Homeland Security and Department of Transportation	The transportation sector moves people and goods. It includes aviation, highway and motorway, maritime, mass transit and passenger rail, pipeline systems, freight rail and postal and shipping.
Water and Wastewater Systems: Environmental Protection Agency	The water and wastewater systems sector is responsible for the nations clean water supply. It also is critical in the management of sewage and wastewater treatment.

To better prioritize resources and focus, and aid in the rapid recovery from all hazards the National Infrastructure Protection Plan (NIPP) identifies communications, energy, transportation and water management as lifeline functions (Department of Homeland Security, 2013: 17). Identification of these functions within a critical infrastructure sector enables stakeholders to better prepare by prioritizing considerations of these functions and by understanding the interdependencies between sectors. Interdependencies refer to the effect an incident in one sector can have on another. For example, in the event of a large scale power outage, how will the lack of grid power affect transportation, wastewater management and so on. Interdependencies and the requirement for intersectoral cooperation will be discussed in greater detail in another section of this chapter.

Identification of lifeline functions is critical in the development of state, local tribal and territorial (SLTT) response and recovery plans. Threat analysis and vulnerability assessments must consider the effect on each of the functions within a sector to identify the prioritization of response and recovery assets. A comprehensive analysis of the loss of energy during a pandemic crisis would emphasize the need for backup power generation at key medical facilities, for example. It would also help planners to understand the effect on communications and water delivery resulting in plans to mitigate the negative effects of losing capability in this lifeline function. Focus on lifeline functions helps to create a foundation for Critical Infrastructure Protection and helps to delineate the responsibilities for all stakeholders.

Threats to the nation's critical infrastructure fall into five categories: direct enemy attack, cyber threats, accidental or technical failures, extreme weather and pandemics (Department of Homeland Security, 2013: 8). A particularly important lifeline sector is energy. The importance of electrical energy in daily life is obvious and often taken for granted. Events or actions in any single threat category could result in significant disruption to the electric energy distribution system. Combined attacks in multiple threat categories could result in catastrophic, long-term loss of electric power. Enemies of the US could look for or facilitate widespread grid outages and exploit degradation in communications, commitment of security resources to domestic recovery, disruptions in food, water and health service delivery and attack when the US is weakened.

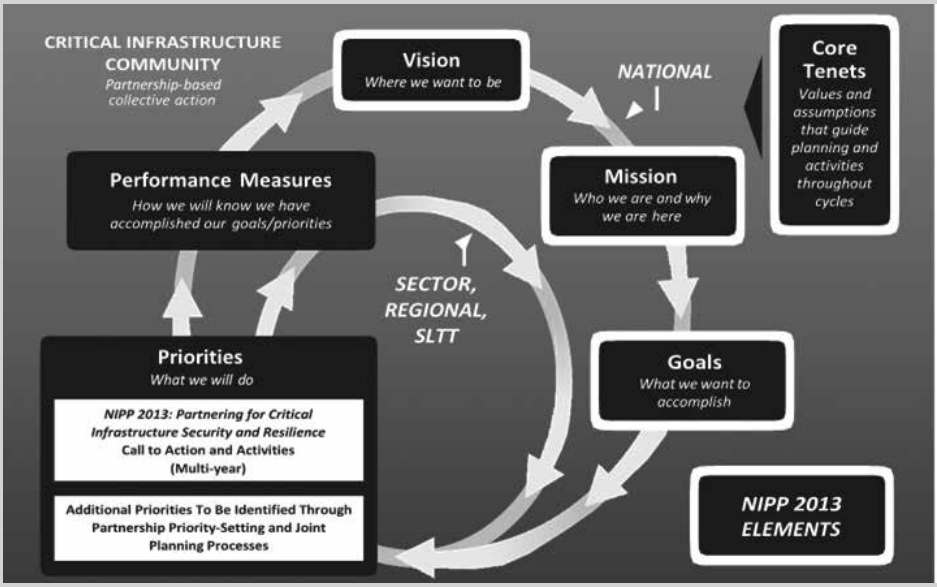
Exacerbating the vulnerability of America's critical infrastructure is the fact that no single organization has authority over it (Association of Old Crows and others, 2014: 5). No matter how diligent critical infrastructure owners are, the achievement of a cohesive, synchronized effort to protect the vast number of interdependent portions will likely not be fully achieved. Enabling individual citizens willing to take greater control where they realistically can will help to strengthen the overall effort. It is estimated that approximately 85 % of critical infrastructure is privately owned (United States Government Accountability Office, 2009). Protecting the nation's infrastructure to include the electric grid requires cooperation and communication among all the stakeholders, governments, private industry and local communities. Although governments regulate many aspects of power production and distribution, private industry, public commissions and cooperatives along with the average citizen must collaborate to establish vital elements of resiliency and

security. In the next section we will discuss the relationship between government at the federal, state, local, tribal and territorial levels and the private sector owners of critical infrastructure.

4.2. Public-Private Partnerships: The Roles and Responsibilities of Critical Stakeholders

The critical infrastructure protection in the United States is a shared responsibility between private sector owners in each sector and governmental agencies at the Federal, State, Local, Tribal and territorial levels. The United States Government Accountability Office (GAO) estimates that 85 % of the nation's critical infrastructure is owned by the private sector (United States Government Accountability Office, 2009). The U.S. government, in coordination and collaboration with key stakeholders has developed a number of standardization documents that provide structure to protection programs across the breadth of the 16 sectors.

Figure 2:
The United State's Plan's Approach to Building and Sustaining Unity of Effort



Source: NIPP, 2013

The 2013 USA National Infrastructure Protection Plan, maintains the task from previous versions of the National Plan for The Department of Homeland Security to maintain sectoral plans for all critical infrastructure sectors that represent a cross-section of sectoral policies, measures and activities of all involved sectoral factors. The first such sectoral plans were adopted in 2010 and revised in 2015. Each of them is additionally linked to specific strategic security policy documents. Sector specific policy can only be executed through voluntary collaboration with private sector owners and operators and their government counterparts. The Government and private sector each have unique responsibilities and the perspectives of each

are equally important. Sectoral Specific plans are maintained through the use of Sector Coordinating Councils, Government Coordinating Councils and Regional Consortia. These collaborative bodies are further broken down to focus on specific areas within a sector. For example, in the Financial Services sector, the Financial Services – Information Sharing and Analysis Center (FS-ISAC) acts as the financial industry "go to" resource for cyber and physical threat intelligence analysis and sharing. This is a membership based organization comprised of private sector, government, non-profit and select partner stakeholder organizations. ISACs are established in other sectors as well. The National Council of ISACs is a coordinating body that facilitates the collaboration of sector-based ISACs. A complete list of all operating sector based ISACs can be found at the NCI website: https://www.nationalisacs.org. ISAC members contribute sector specific information and intelligence in an effort to benefit from sector-wide knowledge and experience. This voluntary collaboration among sector stakeholders is a key element in the overall National Critical Infrastructure Protection Plan and is vital to successful Critical Infrastructure Protection efforts.

The overarching guidance for protection of the Energy Sector is the United States National Infrastructure Protection Plan. As part of the National Infrastructure Protection Plan, the public and private sector partners in each of the 16 critical infrastructure sectors and the state, local, tribal, and territorial government community have developed a Sector-Specific Plan that focuses on the unique operating conditions and risk landscape within that sector. Developed in close collaboration with federal agencies and private sector partners, the Sector-Specific Plans are updated every four years to ensure that each sector is adjusting to the ever-evolving risk landscape. In 2015 sector specific updates addressed the nexus between cyber and physical security, interdependence of sectors, risks associated with aging infrastructure, outdated technology and climate change and the changes in the workforce needed to continue to support the National Plan.

Lifeline Sector Plan Overviews

Energy

In 2013, PPD-21 identified the Energy Sector as uniquely critical because it provides an essential function across virtually all critical infrastructure sectors. The most recent Sector-Specific Plan for the Energy Sector is the 2015 edition (Department of Homeland Security, 2015a). The lead agency for the Energy Sector plan is the US Department of Energy (DOE). The Energy sector update was a collaborative effort between the DOE, the Energy Sector Coordinating Councils and government partners. The interrelated sub-components for the Energy Sector are Electricity, Oil and Natural Gas. This includes the production, refining, storage and distribution of electricity, gas and oil. It does not include the production of hydroelectric or nuclear power. These specific sources fall under separate sub-sectors. The Energy Sector supports the transportation industry, supplies electricity to businesses and neighborhoods and provides power to industrial and agricultural production across the United States. It is in turn dependent on information technology, communications, water and finance as well as other aspects of the Critical Infrastructure sectors.

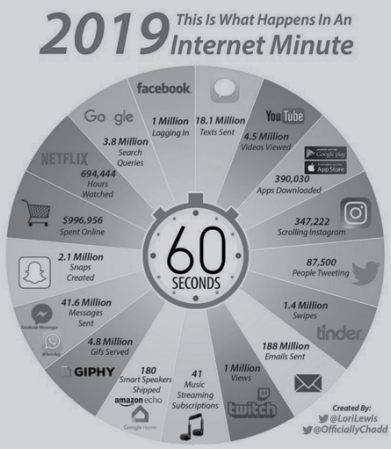
A key component of the sector specific plan is the assessment of threats and risk. The Energy sector plan identifies risk and threat in each of the sub sectors. For the Electricity sub-sector the 2015 plan highlights cyber and physical security threats; natural disasters and extreme weather conditions; workforce capability and human error; equipment failure and aging equipment; evolving environmental, economic and reliability regulatory requirements and changes in the technical and operational environment as the primary threats and risks. Similarly in the Oil and Gas sub-sectors, natural disasters and extreme weather; regulatory and legislative changes – including environmental health; volatile oil and gas demand; operational hazards; political and civil unrest and terrorist activity; transportation infrastructure constraints; inadequate and unavailable insurance coverage; aging infrastructure and workforce and cybersecurity risks and insider threat as primary areas of threat and risk.

Communications

The nature of communications has changed significantly in the past 25 years moving from a primarily voice services oriented environment to an interconnected industry using terrestrial, wireless and satellite communications systems. The Communications Sector Coordinating Council and the Communications Sector Government Coordinating Council worked collaboratively to update the 2010 Communications Sector Specific plan. The plan recognizes the importance of private sector participation in that most communications infrastructure in the US is privately owned and operated. In the 2015 plan the sector identifies 3 goals:

1. Protect and enhance the overall physical and logical health of communications.
2. Rapidly reconstitute critical services in the event of disruption and mitigate cascading effects.
3. Improve the sector's national security and emergency preparedness posture with Federal, State, local, tribal, international and private sector entities to reduce risk (Department of Homeland Security, 2015b: iv).

Figure 3: Internet data every minute



Source: Cyber Security Hub via Linkedin

The sector specific plan update provides targets for public and private partner collaboration among government agencies and private industry. The Communications sector provides products and services that are necessary to the function of other critical infrastructure sectors. They involve both physical infrastructure such as switches, towers and antennas as well as cyber infrastructure such as switching software, applications and operational support architecture. Virtually every aspect of modern life depends upon the cyber infrastructure. Banking, goods and services, emergency communications

and day to day personal interaction are now dependent on a resilient and reliable cyber network. This dependence makes it critical for public-private partnership that addresses all-hazard threats across all aspects of the sector and at all levels of responsibility, to include that of the individual.

The amount of data that is transmitted via the internet every minute emphasizes the reliance modern societies have on the communications infrastructure of not only the US but globally. According to Ericsson (2019), mobile data usage in North America has increased by 40% since 2015. It is projected that this exponential growth will continue with increased capacity of smart devices as well as flexibility of service plans.

With the continued growth of the number and types of devices and the supporting architecture to support them is the necessity for new and emerging policy that protects the infrastructure and more rapidly identifies threats and vulnerabilities. Sector partners must continue to collaborate and evolve to meet this increasing need.

Risk assessment is a key part of the sector specific plan. The Communications Sector plan update for 2015 identifies the following areas within its risk profile:

- Natural disasters and extreme weather – hurricanes and wildfires are among the events that have increased in frequency in recent years. Geomagnetic storms are also on the list of natural events that could cause widespread collapse of power grids and cause long-term outages to national communications.
- Supply chain vulnerabilities – the sector is reliant on hardware and software and the suppliers that provide them to the industry.
- Global political and social implications – geopolitical unrest, economic conditions both foreign and domestic can negatively impact the sector.
- Cyber vulnerabilities – the proliferation of malicious activity to disrupt or deny internet access, data access and data integrity is an on-going concern.

The Communications sector is one of the few sectors that can affect all other sectors. The stability and reliability of the sector facilitates the stability and reliability of the system as a whole.

Transportation

The 2015 update represents the maturation of the sector's partnerships and describes an approach to manage security and resilience in the nation's transportation systems. It balances the freedom of movement of goods and people with the potential loss of civil liberties that could result from over regulation and restrictions. Transportation systems provide lifeline services for the movement of commodities and the ability to respond and recover from disasters. The Transportation Sector, Sector Specific Plan (TS SSP) identifies 4 goals:

1. Manage the security risks to physical, human and cyber elements of critical transportation infrastructure.
2. Employ the sector's response, recovery and coordination capabilities to support whole community resilience.

3. Implement processes for effective collaboration to share mission-essential information across sectors, jurisdictions and disciplines as well as between public and private stakeholders.
4. Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard US national interests (Department of Homeland Security, 2015c: iv).

The TS SSP recognizes advances in efforts to upgrade cyber security to align with growing concerns regarding cyber threats and their effects. It considers an all-hazards approach to resiliency and preparedness across aviation, maritime, freight rail, highway and motor carrier, pipeline, postal and shipping and mass transit transportation systems domestically and internationally. Similar to other sectors, transportation is primarily facilitated by private sector companies. Its owners and operators assess risk and develop plans to mitigate risk and respond to disaster. These plans are developed collaboratively via the numerous coordinating councils and partnership councils facilitated by both government sector and private sector agencies. The US Department of Homeland Security is the primary responsible agency for sector plan development and coordination and within it's span of control shares responsibility with the US Department of transportation, Transportation Security Administration (TSA) and the US Coast Guard (USCG). Government coordinates with industry through regional councils, professional and academic organizations and informal information sharing conferences and knowledge events. Information sharing is the foundation to collaboration among stakeholders. The Transportation Security Information Sharing Environment plan listed multi-directional sharing; effective and efficient processes; trusted partnerships; security education, training and awareness and protection of private liberties as the key goals of the plan. To address growing concerns regarding cybersecurity in the transportation sector, the Transportation System Cybersecurity Working Group was established. It is comprised of Federal, SLTT and private industry representatives. This group raises general industry awareness, promotes community actions and fosters collaborative approaches to heightening overall cybersecurity across the entirety of the transportation sector.

Risks to transportation critical infrastructure include manmade and natural events. Man-made threats include terrorism, both physical and cyber. Aging infrastructure results in higher probability of catastrophic destruction to physical infrastructure due to severe weather, vandalism, sabotage and technological failure. Natural disasters, climate change and extreme weather events can destroy and or degrade transportation systems. Floods, wildfires blizzards hurricanes, tornadoes and droughts all affect transportation services. In the spring of 2019, droughts in Central America resulted in lower water levels in the Panama Canal. Lowered water levels restrict the size of ships that can navigate through the canal. This results in loss of revenue for the canal operators, reduction in quantity that can move through the canal and in extreme events, restrictions in the types of vessels that can navigate the canal (Zamorano and Franco, 2019).

The continued cooperation among all stakeholders and the continuation of extensive information and intelligence sharing through councils and work groups within the sector and in cross-sector events is critical to meeting the ever-changing threat environment.

Water and wastewater

The purpose of the Water and Wastewater Sector Specific Plan (Water SSP) is to secure and strengthen the resilience of the sector's infrastructure (Department of Homeland Security, 2015d). Simply put, the Water and wastewater sector pertains to the maintenance of safe and reliable drinking water systems necessary to maintaining public health and preventing disease. The infrastructure that delivers fresh drinking water and safely transports and treats wastewater is overseen by Federal, state, local, territorial and tribal government entities as well as private sector stakeholders. The Water SSP uses the partnership model outlined in the NIPP to bring private and public sector leaders into the planning and implementation of sector protection efforts. The US Environmental Protection Agency (EPA) is the government agency with primary responsibility for the sector.

The safety and reliability of the nations drinking water system is paramount to health, economic, psychological and environmental concerns nationwide. Events such as the contamination of drinking water systems such as the Flint Michigan water supply contamination event highlight the drastic human health issues caused by negligence in addressing possible contamination (NRDC, 2018). In an effort to save money, city officials decided to discontinue using fresh water piped in from Detroit and instead would use water sourced from the Flint River until a new pipeline from Lake Huron could be built. The city failed to properly decontaminate and purify this supply which resulted in significant increases in blood lead levels in children, skin rashes and numerous other ailments. An effort to save money resulted in significant extra costs to not only clean up the water supply and delivery systems but to compensate Flint residents for their medical and health related expenses.

The Water SPP is a guiding document to help eliminate events such as that experienced in Flint, Michigan. In addition to the human element, the plan considers numerous elements in the drinking water category. Water source, conveyance, raw water storage, treatment, finished water storage distribution systems and monitoring systems comprise the physical components addressed in planning. Supervisory Control and Data Acquisition (SCADA) systems and Process systems and operational controls are areas of emphasis under cyber elements. The control and management of distribution and production are increasingly controlled by digital systems. Compromise of these systems is an identified threat.

Wastewater is addressed separately in the Water SPP. The physical element of the wastewater portion of the plan consists of collection, raw influent storage, preliminary treatment, treatment, disinfection, effluent/discharge, residual and biosolids and monitoring systems. The cyber element involves the same areas as identified in the water sections, SCADA and process systems and operational controls. Of course the human element has to be considered. Not only are the public officials but also laboratory technicians, microbiologists, chemists, public works employees and environmental specialists to mention a few of the professionals necessary to administer this complex system.

Sector risk is categorized as Most Significant, High, and Medium risks. Most significant threats require prioritized attention and mitigation. They pose the

greatest potential for high impact. High risk requires serious attention whereas medium risk events could escalate without thoughtful attention. Examples of Most significant risk are natural disasters such as floods, earthquakes and other natural events that negatively impact water quality for large geographic areas, aging infrastructure and associated economic implications and the possibility of escalating consequences resulting from the inability to manage a crisis across a large area. High risks can be deliberate malicious acts, inaction from stakeholders or utilities and inadequate preparation, response and recovery. Medium risks are insufficient or improper management of assets and resources and a lack of planning in emergency response and mutual aid. These examples of how risk is categorized help to create prioritization based on recognized need across the sector. Risk analysis is situationally dependent and the context of risk analysis outlined in the SSP helps to contextualize the process required to evaluate unique situations.

Sector specific plans exist for all of the 16 sectors. An outline of the Sector Specific Plans provides a general understanding of the detail that each sector specific agency must facilitate in order to address the complexity of each sector. As demonstrated throughout this section, the necessity for collaboration among all stakeholders in each sector cannot be over emphasized. Regular interaction whether formally or informally is required to address the dynamic nature of technology, threat and vulnerability. Plans must be flexible and agile and contain policy that enables adaptation with oversight.

4.3. National standards and the Role of the Government in Policy and Enforcement

The US government began to formalize efforts to develop a comprehensive national policy for Critical Infrastructure in the mid-1990s. *Executive Order (EO) 13010 Critical Infrastructure Protection,* 1996 states that "certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." Threats to Critical Infrastructures are primarily determined as physical and cyber (The White House, 1996). The EO further establishes bodies and accompanying mechanisms with the aim of developing a normative framework for critical infrastructure protection in the United States. Among others, it established the President's Commission on Critical Infrastructure Protection (PCCIP) composed of both public and private sector representatives, and charged them to assess the threats and vulnerabilities to the Nation's infrastructure and to recommend national policy and a strategy for protection. In July 1996, President Clinton established the Commission on Critical Infrastructure Protection (PCCIP), with a charter to designate critical infrastructures, to assess their vulnerabilities, to recommend a comprehensive national policy and implementation strategy for protecting those infrastructures from physical and cyber threats, and to propose statutory or regulatory actions to affect the recommended remedies. The PCCIP submitted its report, *Critical Foundations: Protecting America's Infrastructures,* in October 1997. The PCCIP report was the basis for Presidential Decision Directive 63 (22 May 1998), *Critical Infrastructure Protection,* which establishes national policy and an organizational structure for effecting a

public-private partnership and for accomplishing the special protection functions that are inherently the responsibility of government (Department of Defense, 1998). Critical Infrastructure was defined in 1998 *Presidential Decision Directive / NSC-63 Critical Infrastructure Protection* as "physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private." Further, it is emphasized how "[m]any of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber-attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security" (The White House, 1998).

Presidential Policy Directive 21 (PPD 21) articulates the primary responsibilities of the US Federal Government's role in strengthening the security and resilience of US Critical Infrastructure against physical and cyber threats. PPD 21 emphasizes the need for partnership with private sector and international stakeholders and recognizes the interdependent nature of the critical infrastructure system as a whole (The White House, 2013). The federal government facilitates regulatory compliance through regular communication, inspection programs, licensing requirements and financial penalties for non-compliance.

To assist state and local governments with implementing the National Infrastructure Protection Program (NIPP), the Department of Homeland Security (DHS) has implemented a program which uses "Protective Security Advisors". According to the United States Government Accountability Offices (GAO-18-62 Critical Infrastructure Protection), DHS PSA program was established in 2004 to assist with ongoing state and local CI security efforts by establishing and maintaining relationships with state Homeland Security Advisors, State Critical Infrastructure Protection stakeholders, and other state, local, tribal, territorial, and private-sector organizations. PSAs are to support the development of the national risk picture by conducting vulnerability and security assessments to identify security gaps and potential vulnerabilities in the nation's most critical infrastructures (United States Government Accountability Office, 2017).

While useful and a large improvement over earlier, disconnected or inconsistent efforts to implement a national level program , through obtaining local level information, the PSA role is still to focus on the National Level, while assisting with and supporting the state, local, tribal and territorial efforts. PSAs are a tremendous help in making the connection between the local level governments and the CI owners/operators. They serve as subject matter experts on the NIPP and are most often, the representative of DHS CIPP efforts that is most well-known by state and local officials.

Following the release of PPD-21 and Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity*, the Interagency Security Committee (ISC)

established a working group to review The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard and evaluate its effectiveness pertinent to strengthening the security and resilience of Federal critical infrastructure. EO 13636 further directed the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cybersecurity risks to critical infrastructure. In February of 2014, National Institute of Standards and Technology (NIST) published the *Framework for Improving Critical Infrastructure Cybersecurity.* The framework was further revised and in 2018 Version 1.1 of the document was released. The primary purpose of this document is to provide business and government a common framework using common language that identifies cybersecurity risk and facilitates the implementation of practices and policies to identify vulnerabilities and reduce the risks those vulnerabilities pose. It also outlines methodologies for categorizing risk and risk tolerance. The commonality of the framework and use of globally recognized standards allows for the Framework to stand as a model for international cooperation across all sectors (National Institute of Standards and Technology, 2018).

In 2017, the White House issued an Executive Order focused on continuing to strengthen efforts in CIP – particularly for Cybersecurity of Federal Networks and support to CI owners/operators. The Executive Order directed all Federal Departments to "use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk" (White House, 2017).

The directive further orders key departments and agencies to *"identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities"* (White House, 2017). Clearly, the US continues to view Critical Infrastructure Protection as a key element of National Security.

Throughout this discussion, it has been emphasized the importance of the private sector involvement in CIP policy and action. US Governmental oversight relies upon the involvement and input from industry. Through the many coordinating councils and sector specific information sharing organizations, sector stakeholders develop standards and operational best practices to which they generally hold themselves accountable. This is not to say that the Federal, State, local, territorial and tribal governments do not implement laws, rules and regulations governing the conduct of activity related to Critical Infrastructure. At all levels of government in the US, agencies implement legislation that guides and directs the operations of owner-operators across all 16 sectors. To provide a comprehensive list of all the governing documents is not realistic for this text but a highlight of the nature of a few can be used to illustrate how regulation shapes activity relating to CIP.

The National Infrastructure Protection Plan 2013 is the overarching document that outlines the vision, mission, goals and core concepts for both government and public-private owner-operators of critical infrastructure. It creates the structure in which partnerships measure against established goals and associated metrics. Sector-specific plans, as previously identified, further refine goals and objectives and

refine information relevant and current to specific sectors. Standards organizations such as NIST develop even greater detail in the way of specific operating practices. Although NIST is a non-regulatory agency, standards developed by NIST create benchmarks by which organizations are measured to determine their ability to securely provide goods and services. The US Federal government uses these standards in the awarding of government service contracts. Private sector organizations that do not demonstrate NIST compliance in areas of concern, such as cyber security, do not meet the basic requirements for consideration in the contracting process. This concept exists for numerous other organizational and industry standards. A detailed list of organizations and the industries they serve can be found by visiting the American National Standards Institute (ANSI) website.[4] The following is a short list of a few of the larger organizations that cross many Critical Infrastructure sectors:

1. NSF International. NSF is a non-governmental, not-for-profit organization that is internationally recognized in the public health and safety field. This organization provides training and certification in a wide variety of disciplines related to public health and safety.[5]
2. ASME (American Society of Mechanical Engineers). ASME is a not-for-profit professional association that promotes the practice of mechanical and multidisciplinary engineering practices throughout the world. Over 500 ASME technical standards are recognized globally for nuclear power components, piping systems, valves cranes and pressure containers among other areas.[6]
3. ISO (International Standards Organization). ISO is a nonprofit organization that develops and publishes standards of virtually every nature. It is headquartered in Geneva, Switzerland represented by 162 members each representing their home country. ISO is the largest developer and producer of standards in the world.[7]
4. FINRA (Financial Industry Regulatory Authority). FINRA is a not-for-profit organization authorized by the US Congress to protect investors by ensuring the broker-dealer financial market operates fairly and honestly. FINRA is a collaborative organization that writes rules governing investment dealings, conducts examinations of firms to ensure compliance and provides investor education. FINRA licensed dealer-brokers must adhere to rigorous standards to protect US financial investment markets.[8]
5. US Department of Transportation (DOT) standards. The US DOT oversees the nation's highways and waterways. This agency provides a comprehensive program involving regulation, production standards, operating standards

4 ANSI provides information on Standards Developing Organizations that work to conform best practices across numerous industries that work within the 16 sectors of Critical infrastructure. Although not tied directly to the National Plan, many standards and organizations play a critical role in ensuring the highest standards of quality and safety are maintained in both the public and private sectors. See more at https://www.standardsportal.org/usa_en/resources/sdo.aspx

5 Detailed information regarding NSF International standards and programs can be found at http://www.nsf.org/

6 Detailed information regarding ASME and ASME standards can be found at http://www.asme.org/

7 Details regarding ISO and their programs can be found at https://www.iso.org

8 FINRA provides a wide variety of tools and services within the financial sector. A comprehensive understanding of their regulatory activity and licenses are available at https://www.finra.org

and general rule making in the greater scope of the transportation sector. DOT collaborates with non-governmental standardization organizations in numerous areas to ensure the nation's transportation system is safe and efficient. DOT areas of focus include automobiles, aviation, bicycles and pedestrians, public transit, pipelines and hazardous material, trucking and motorcoaches, maritime and waterways and roadways and bridges.[9]

6. HIPAA (Health Insurance Portability and Accountability Act). The HIPAA Act of 1996 established standards for the protection of individuals medical records and other personal health information. HIPAA requirements apply across sectors that involve public health and the transmission of personal health information.[10]
7. North American Electric Reliability Corporation (NERC). NERC standards apply to bulk energy producers in North America. The standards focus on performance, risk management and entity capabilities.[11] NERC standards define the reliability requirements for operating bulk power systems. NERC develops standards through the use of a standards committee comprised of representatives from all aspects of the energy production and distribution system, both the private sector and public sector. NERC facilities compliance and enforcement of standards and regulates the North American power grid and the owner-operators that comprise the power generation and distribution system.

These are a few of the high profile organizations that establish and enforce standards that span all aspects of the national Critical Infrastructure system. It is a collaborative that involves government agencies, not-for-profit organizations, industry professionals and academic institutions. Only through participation from all parties can the broad and dynamic nature of the nation's Critical Infrastructure be addressed, maintained and secured.

4.4. Critical Infrastructure Sector Interdependency

The 16 Critical Infrastructure sectors cannot be considered independently. Each sector has a linked dependency to other sectors. Understanding the relationships between sectors and the sub-components of sectors and how they mutually support other sectors enables a comprehensive approach to identifying risk and mitigating responsibilities.

There is reasonable concern that national and international energy and information infrastructures have reached a level of complexity and interconnection that makes them particularly vulnerable to cascading outages, initiated by material failure, natural calamities, intentional attack, or human error. The potential ramifications of network failures have never been greater, as the transportation, telecommunications, oil and gas, banking and finance, and other infrastructures depend on the continental power grid to energize and control their operations.

9 A complete list of responsibilities, activities and processes are available at the Department of Transportation website. https://transportation.gov.

10 HIPAA privacy rules and how they apply to various industries can be found at the US Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

11 Standards, NERC.com 2019. https://www.nerc.com/pa/Stand/Pages/default.aspx

Each of the previously mentioned sectors can be seen as a certain "level above" typical Critical Infrastructure in terms of the importance of the service/function provided. The degree to which our modern society relies on these particular sectors supports their designation as "lifeline sectors" for critical infrastructure.

A growing portion of the world's business and industry, art and science, entertainment, and even crime are conducted through the World Wide Web and the Internet. But the use of these electronic information systems depends, as do the more mundane activities of daily life, on many other complex infrastructures, such as cable and wireless telecommunications; banking and finance; land, water, and air transportation; gas, water, and oil pipelines; and the electric power grid.

Taken individually, or in the aggregate, all these systems are intimately linked with the economic well-being, security, and social fabric of the communities they serve. Thinking about critical infrastructure through the subset of lifelines helps clarify features that are common to essential support systems and provides insights into the engineering challenges to improving the performance of large networks.

Lifeline systems are interdependent, primarily by virtue of physical proximity and operational interaction. Lifeline systems all influence each other. Electric power networks, for example, provide energy for pumping stations, storage facilities, and equipment control for transmission and distribution systems for oil and natural gas. Oil provides fuel and lubricants for generators, and natural gas provides energy for generating stations, compressors, and storage, all of which are necessary for the operation of electric power networks. This reciprocity can be found among all lifeline systems (O'Rourke, 2007).

The most important directive for current Critical Infrastructure Protection in US policy, is Presidential Policy Directive (PPD) 21. Following the recommendations adopted in PPD-21, the 2013 NIPP affirms that "effective risk management requires an understanding of the criticality of assets, systems, and networks, as well as the associated dependencies and interdependencies of critical infrastructure" (Department of Homeland Security, 2013).

Assessment of critical infrastructure dependencies and interdependencies is one of the seven core tenets defined in the 2013 NIPP. According to the plan, "understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience" (Department of Homeland Security, 2013). These strategic directives reveal the importance of analyzing infrastructure dependencies, interdependencies, and associated cascading effects from critical infrastructure disruptions to improve national security and resilience.

The directive also highlights the importance of lifeline critical infrastructure dependencies, noting the need to consider "sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems" (The White House, 2013).

Evolving theories regarding infrastructure protection includes viewing infrastructure systems as complex interactive networks (Amin, 2000). Increasing interactions take place between this infrastructure and the electric power grid;

size and complexity continues to increase at a rapid rate. The occurrence of several cascading failures in the past has helped focus attention on the need to understand the complex phenomena associated with these interconnected systems.

Many of our nation's critical infrastructures are complex interdependent networked systems; prime examples are the highly interconnected and interactive industries, which make up a national or international infrastructure, including telecommunications, transportation, gas, water and oil pipelines, the electric power grid, and the collection of satellites in earth orbit. Interactions between networks such as these increase the complexity of operations and control. Secure and reliable operation of these systems is fundamental to our economy, security and quality of life. These large scale networks are characterized by many points of interaction among a variety of participants-owners, operators, sellers, and buyers. The networks' interconnected nature makes them vulnerable to cascading failures with widespread consequences.

Energy, telecommunications, transportation, and financial infrastructures are becoming increasingly interconnected, thus posing new challenges for their secure, reliable, and efficient operation (Amin, 2002). Virtually every crucial economic and social function depends on the secure, reliable operation of infrastructures.

As these infrastructures have grown more complex to handle a variety of demands, they have become more interdependent. The Internet, computer networks, and our digital economy have increased the demand for reliable and disturbance-free electricity; banking and finance systems depend on the robustness of electric power, cable, and wireless telecommunications. Transportation systems, including military and commercial aircraft and land and sea vessels, depend on communication and energy networks. Links between the power grid and telecommunications and between electrical power and oil, water, and gas pipelines continue to be a lynchpin of energy supply networks. This strong interdependence means that an action in a part of one infrastructure network can rapidly create global effects by cascading throughout the same network and even into other networks.

Cross-Sector Measures and Collaboration

The evolution of the cross-sector collaboration and cooperation in CIP in the US includes the development of the Critical Infrastructure Cross-Sector Council. The CI Cross-Sector Council is the private sector organized and managed representative critical infrastructure cross-sector council. Developed in 2015, the CI Cross-Sector Council facilitates consultations, information sharing, and coordinated effort across the critical infrastructure sectors and sub-sectors and with the Federal government, as well as with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), the Regional Consortium Coordinating Council (RC3), and the National Council of Information Sharing and Analysis Centers (NCISAC) (Department of Homeland Security, 2015e).

The CI Cross-Sector Council was formed to assure the opportunity to engage with Federal government officials for the purpose of achieving consensus on joint priorities and actions to advance critical infrastructure security, protection and

resilience, joint meetings between the CI Cross-Sector Council and representatives of Federal departments and agencies (Department of Homeland Security, 2015e: 2). The CI Cross-Sector Council is organized and managed by, and responsible to, the leaders and designated representatives of the Sector Coordinating Councils (SCCs) that comprise its membership. The CI Cross-Sector Council provides the representative forum for consultations, coordination, and cooperative efforts on matters pertaining to critical infrastructure security, protection and resilience for its members.

Additionally, the National Infrastructure Advisory Council (NIAC), which serves in an advisory capacity to the President of the United States, recommended in August of 2017 that further studies be undertaken in the area of increased collaboration and cross-sector measures.

The NIAC recommended to the President of the United States that the Council could assist with informing risk reduction activities by further study of the following seven areas:

1. Incorporating resilience into Federal capital planning and recovery investments
2. Using insurance to recognize and reward investment in resilience
3. Public-private, cross-sector, and regional information sharing
4. Cross-sector interdependency risks during long-duration energy disruptions
5. Port infrastructure security and resilience
6. Workforce trends affecting critical infrastructure security and resilience
7. Security and resilience of oil and natural gas transit by pipeline and rail (Department of Homeland Security, 2017a).

As our world becomes more and more connected and our modern marketplace develops faster and more intelligent systems to provide control and management of critical infrastructure, it is a growing challenge that we will be forced to identify and mitigate risk caused by these increasing interdependent and connected systems.

4.5. Future Landscape of Critical Infrastructure in the United States

The Nation's critical Infrastructure and the focus to identify and protect is ever-evolving. From the end of World War II to Pre-9/11 (the attacks on the World Trade Center in New York, USA) the focus has been on the defense industrial base and physical threats posed by actors external to the United States, primarily from nation states. After the World Trade Center attacks, a defining moment much like the attack on Pearl Harbor, the national attention shifted and the vulnerability to terrorist attacks on the nation's infrastructure became more apparent. Through 2007 the focus was on the identification and cataloging of the nation's critical infrastructure assets. From 2007 to 2013 the focus turned to the identification and prioritization of lifeline sectors and the overall interdependency of the critical infrastructure system as a whole. The proliferation of digital information exchange and connected enterprise lead to our current focus, building resiliency and cybersecurity.

The proliferation of connected devices will exponentially increase the complexity of protecting critical infrastructure. Automation and autonomous systems present new potential attack surfaces in all sectors. The increasingly interconnected and interdependent nature of CI systems will make cross-sector collaboration a dire necessity.

Critical Infrastructure Protection across the nation at all levels of government and community stakeholders remains a priority and a challenge. The US National Preparedness Report (NPR) findings from 2017 indicate that "public and private-sector partners continue to focus on improving infrastructure systems to address vulnerabilities posed by deteriorating critical infrastructure" (Department of Homeland Security, 2017b: 89).

CIPP continues to be a high priority and yet a persistent challenge to US states and local governments. In the 2017 National Preparedness report, summarizing the status of preparedness and security in the United States, the section on Infrastructure Systems provides a concerning assessment on the state of affairs.

The focus of Infrastructure Systems is on stabilizing critical infrastructure functions, minimizing health and safety threats, and efficiently restoring and revitalizing systems and services to support a viable, resilient community. While Federal departments and agencies took steps to address challenges to this core capability, as detailed on page 89, limited evidence exists demonstrating that the Nation has made significant progress in this area. Aging infrastructure in many sectors presents growing risks, as well as decreases resilience …States and territories identified this core capability as exhibiting below-average levels of proficiency in 2016 (Department of Homeland Security, 2017b: 14).

Regardless of the approach, there needs to be a basic understanding of the elements that make up the system. A challenge for future researchers, whether academic, private sector, or government institutions, is to develop a "maturity model" to evaluate local CIP efforts and a guide towards a more fully robust and mature risk reduction and resilience model. Critical Infrastructure Protection must continue to evolve to meet the dynamic nature of maturing societies, the changing needs of its people and the development of new and yet to be seen technologies. An agile, adaptive and integrated methodology that uses all system stakeholders is the only way to ensure a resilient and reliable Critical Infrastructure Architecture.

Chapter conclusion

This chapter looked at five aspects of Critical Infrastructure Protection. In section one, the general structure of US Critical Infrastructure Protection was outlined. This section discussed the sixteen Critical Infrastructure Sectors and identified the governmental agencies with primary responsibility for policy, oversight, strategic planning, security collaboration and enforcement. Section two discusses the public-private nature of critical infrastructure ownership and oversight and identified some of the formal collaborative group established to bring stakeholders together to work through the evolving challenges the nation faces to secure its critical infrastructure. Section three discusses the structure of National Standards that create the frameworks used to establish consistency across sectors and to create a

common language for all stakeholders in all sectors. Section four builds on section three by discussing the interdependent nature of the sixteen critical infrastructure sectors and identified the further designation of life-line sectors. Since the sectors cannot be considered independently, the structure of National Standards and National Frameworks like the NIST Cybersecurity Framework ensures cross-sector standardization and helps to model the nature of potential cascading effects of events originating in one or more sectors. Finally, the chapter looked at the future landscape for Critical Infrastructure Protection with a brief discussion of the impact of cyber events, the proliferation of connected devices and the ease of disruption by non-state actors in a changing and evolving geopolitical landscape.

The way forward for Critical Infrastructure Protection and practitioners in the field is complex and ever-changing. The need for collaboration and partnership across sectors and between the private sector and public sector stakeholders will become more imperative. As everyday life becomes more connected and average people depend more of autonomous services and interconnected devices, the role of the individual in Critical Infrastructure Protection will also become more important. Any system is only as secure as its weakest point. A strong Critical Infrastructure Protection plan encompasses all possible vulnerabilities and weaknesses, to include the human being.

CHAPTER 5

CRITICAL INFRASTRUCTURE PROTECTION IN CROATIA

CHAPTER 5

Critical Infrastructure Protection in Croatia[12]

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

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

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

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

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

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

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

5.1. The period until the entry into the European Union

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

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

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

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

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

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

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

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

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

First Cycle – Year 2013

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Second Cycle – Year 2014 to 2015

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Third cycle – 2016 – 2018

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

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

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

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

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

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

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

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

With regard to the establishment of cyber security, based on *National Cyber Security Strategy* of 2015, in 2018 *Cyber Security Act of the Key Service Operators and Digital Service Providers* was adopted, which regulates the rights and obligations of the stakeholders of the system concerned and within the criteria are adopted, set out in Annex 1. *A list of key services with criteria and thresholds to determine the importance of the negative impact of the incident* (Croatian Parliament, 2018). With this Act, the *Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)* has been transposed into national legislation. Upon the adoption of the Act, the procedure for identification and prescribed measures for the protection of communication and information infrastructure was established in the Republic of Croatia, and certain Key Service Operators and Digital Service Providers were identified within the legal deadline. The mentioned Act and the processes conducted under its framework are in this initial stage a positive example of how things needs to be done. The experience of the processes that took place under the aegis of the *Critical Infrastructure Act* has certainly contributed to that. For the period in front of us (and it is a short-term consideration of the year or two) it is left to see how processes within these two legislative frameworks will be harmonized, where there will be challenges in overlapping and how it will they be resolved.

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

5.3. Structural Challenges in Establishing a Critical Infrastructure Protection System

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter conclusion

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

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

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

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

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

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

CHAPTER 6

REPUBLIC OF NORTH MACEDONIA AND CRITICAL INFRASTRUCTURE PROTECTION

CHAPTER 6

Republic of North Macedonia and Critical Infrastructure Protection

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

Modern security threats assume a new "innovative" dimension that requires expanding the scope and understanding of certain security threats that can negatively affect the functioning of critical infrastructure. In doing so, they become more sophisticated and more destructive in its manifesto. Such a situation eminently emphasizes the need to develop a modern concept of national resistance and a modern concept for critical infrastructure protection.

In this chapter, the authors refer to the current situation in the Republic of North Macedonia related to the building of an effective system for critical infrastructure protection. Priority sectors, such as energy, information technologies, water systems and air transport have been identified. As a result of the country's reform efforts, in each of the sectors indicated, there are certain legal and secondary legislation that can enable efficient regulation of critical infrastructure protection. Consequently, the authors offer appropriate measures and recommendations that would be most appropriate in the organization of critical infrastructure protection. For instance, an example is provided for creating an effective strategy for critical infrastructure protection. After identifying the existing risks, the strategy should give the right direction to overcome the situation regarding the lack of positive legislation on critical energy infrastructure. However, partial solutions in different critical infrastructure sectors have been identified, though not wrong, are likely to contribute to the "suppression" of the whole process for creating and effectively functioning of the optimal system for critical infrastructure protection. At the end of the chapter, as a result of such conditions, recommendations are given for taking practical steps in the direction of building a critical infrastructure protection system.

6.1. Conditions in the Republic of North Macedonia in the Field of Critical Infrastructure Protection

As a result of the Euro-Atlantic commitments, the Republic of North Macedonia undertakes and realizes a great deal of reforms that inevitably affect the spectrum of issues related to critical infrastructure protection. After its independence, the Republic of North Macedonia began to pursue its own autonomous policy in all

domains of social life, as an equal international legal entity. In that direction, it builds its own principles of foreign policy, as well as security policy principles within that framework, as an inseparable part in realization of own national interests.

In the line of the most important activities, including critical infrastructure protection one can list the following:

- defining objects as critical infrastructure;
- defining measures for their protection and safety;
- defining tasks and responsibilities.

From this aspect, it is of particular importance to note that the determination of critical infrastructure in the Republic of North Macedonia is not in accordance with the guidelines of the European Union. In that sense, there is a lack of clear specification of the critical infrastructure term. Therefore, it is generally accepted that in the specification of objects as critical infrastructure, one should start from the analysis of several decisions, as follows:

- Decision on determining persons and objects for protection. This Decision was adopted based on the Internal Affairs Law. The Decision precisely lists the objects of interest for the security of the Republic of North Macedonia, such as: electric power, postal and shipping, railways, airports, water supply, etc.
- Decision on determining the legal entities that are obliged to have private security[13] The Decision specifies the protection of legal entities, whose activity includes the following:
- handling radioactive substances or other substances hazardous to people and the environment;
- legal entities registered for production and wholesale of medicines and medical devices;
- legal entities registered for production and trade of flammable liquids and gases;
- legal entities registered for transport of dangerous goods;
- legal entities registered for handling objects and facilities of particular cultural and historical significance.[14]

In order to be able to operatively, professionally and efficiently protect the critical infrastructure in the Republic of North Macedonia, part IV of this Decision defines the obligation for private security of the legal entities, especially when the interest is attaining security of the Republic of North Macedonia. In particular, several sectors have been defined, namely:

- energy (production, transmission and distribution of energy);
- water supply;
- environment;

13 This Decision was adopted by the Government of the Republic of Macedonia in 2013, and the need for its adoption derives from the Law on Private Security from 2012 and the Law on Amending and Supplementing the Law on Private Security, adopted in 2013.

14 Decision on determining the legal entities that are obliged to have private security, "Official Gazette of the Republic of Macedonia", no.106/2013, Article 2

- Macedonian Radio and Television, electronic and print media;
- National Bank of the Republic of North Macedonia and other legal entities registered for carrying out banking activities.[15]

6.2. Protection and Security of Critical Infrastructure in the Republic of North Macedonia

Protection and security of critical infrastructure in the Republic of North Macedonia should be directed towards several key sectors, such as:

- energy sector;
- information technologies;
- water systems; and
- air traffic.

Energy sector in the Republic of North Macedonia is regulated in accordance with the Law on Energy. Here, as a priority, we would highlight strategically the most important companies, such as: "ELEM" (Macedonian Electric Power Plants) and "JSC MEPSO" (Macedonian Electricity Transmission System Operator), which together with their capacities represent the pillar of the energy system. While in the oil industry, "JSC OKTA" has priority in the protection because it has a significant role in the sale, supply and distribution of oil derivatives in the Republic of North Macedonia.

Information Technologies. In this sector, a special emphasis should be placed on the wide range of measures for critical infrastructure security and protection. As priorities, we would single out strategically the most important critical infrastructure, that is: "Makedonski Telekom" and "VIP". These are the companies that, with their entire capacities, represent the pillar of the landline and mobile network and the most sophisticated information technologies.

Water systems in the Republic of North Macedonia are regulated in accordance with the Law on Waters. In this sector, special emphasis should be placed on the wide range of measures for security and protection of surface waters, lakes, reservoirs and springs, water management facilities and so on. To this end, it is necessary to provide:

- availability of sufficient quantities of healthy and clean drinking water;
- supply of healthy drinking water;
- prohibition or restriction of use in case of its contamination;
- taking measures to continuously ensure the quality of drinking water.

Air traffic in the Republic of North Macedonia is regulated in accordance with the Aviation Law. According to this Law, organizations involved in the safety of civil aviation at national level are the following:

- Civil Aviation Agency;
- Ministry of the Interior;

15 Ibid

- Airport operators; and
- Air carriers. (Aviation Law, 2015).

Effective security of this critical infrastructure can be achieved only if several preconditions are met, namely:

- continuous development;
- implementation of legal regulations;
- continuous undertaking of measures, programs and procedures.

Hence, we can conclude that in order to achieve a standardized level of aviation safety, through the body responsible for security (usually the Civil Aviation Agency) it is necessary to adopt the following:

- a comprehensive policy, supported by legal regulations, to be implemented by all entities involved in any civil aviation security structure;
- each of the aforementioned subjects, police services, air carriers, intelligence services, etc, must have clearly defined policies, procedures, standards of action and methods of application in accordance with the guidelines of the state;
- proposal for establishing a National Security Committee and a Committee for Airport Safety;
- other efficient bodies to implement in a coordinated way the policy and standards for implementation of security measures. (Alcheski, 2016: 213-2014).

6.3. An Example of Creating an Effective Strategy for Critical Energy Infrastructure Protection

Assuming that in the domain of critical infrastructure protection, the energy and transport sector will be a priority for the Republic of North Macedonia in the process of EU integration, on this occasion we will make a cross-section and analysis of the situation in the area of energy sector.

The precise definition of energy infrastructure of the Republic of North Macedonia is part of the emphasized reform efforts. As one of the structural elements and an integral part of the critical infrastructure, the energy infrastructure is a subject to numerous measures and activities for its protection. What we must emphasize is the fact that the activities undertaken to secure the energy infrastructure constitute a separate concept, different from the concept of energy security that primarily focuses on politically and economically motivated disruptions in the supply of the corresponding energy resources. The modern concept of protecting the energy infrastructure of the developed countries is relatively new and different from the traditional – defensively focused – way of securing energy infrastructure. It is comprehensive and integrated into the concept of critical infrastructure protection and has an inseparable connection with national security. This means that besides state institutions, all relevant structures from the private sector that manage the energy infrastructure are included. As a result, the modern concept has a serious potential to develop into a ***system*** that drastically reduces the risk of modern security threats.

Generally, despite the fact that in our country there is no positive legislation on critical infrastructure, there is still some kind of protection of the facilities and systems that fall into the critical infrastructure category. Unfortunately, such partial solutions, which are often non-consolidated, are not translated into a system, so in practice some institutions may overlap in competencies or in parallel, and act differently. Hence, the importance of this area is perceived, which in itself is an important security issue, and needs to be regulated accordingly. By adopting appropriate legislation (law, by-laws) first, a clear system would be finally established to define the key terms in this area, identify the basic sectors or areas of critical infrastructure, clearly define and assign the role of the central body for coordination, etc., which will result in the creation of an optimal ***system*** in which all necessary, especially human resources will be located and appropriately utilized and because the critical infrastructure protection necessarily requires planning and implementation of security measures and a prompt and appropriate response to the dangers and possible damages. They should include not only state capacities, which are still limited, but also the enormous resources offered by the private security sector.

Nevertheless, as long as the state does not establish the concrete system for critical infrastructure protection, state authorities must accept the current state, that is, partial normative regulation of this issue. As an example, we emphasized the important sphere of energy and energy infrastructure protection will be analyzed.

If an analysis of several national strategies for critical infrastructure protection of the EU and NATO Member States is made, it will be determined that the interest in protecting energy infrastructure from asymmetric threats or natural disasters is one of the key imperatives of modern democratic states. Therefore, modern states and their energy sectors respond appropriate measures as well as responsibility to guarantee the availability of the necessary quantities of energy resources at any time and without interruption that would imply additional security or economic problems. In this context, the Republic of North Macedonia should not and must not be an exception. As a country with an extremely important geopolitical and geostrategic position in Europe and defined strategic determinations for integration into the EU and NATO, the energy infrastructure of the Republic of North Macedonia is not immune to global asymmetric threats. In the recent history, the Republic of North Macedonia has not yet faced specific security threats and damage to the energy infrastructure that would have serious consequences for its economic and security situation. However, the lack of operational national and legal regulations for prevention, as well as an appropriate response in case of threats to the security of energy infrastructure – as a result of asymmetric threats – has the potential to cause serious consequences for the Republic of North Macedonia and its citizens. Since it is a national security problem, it is obvious that the security of energy infrastructure is primarily the task of the Government of the Republic of North Macedonia but not its single responsibility. To a large extent, this is because many potential terrorist or subversive goals – such as hydro power plants, thermal power plants, Okta refinery, Thessaloniki-Skopje pipeline, the main gas pipeline Deve Bair-Skopje and so on, are owned or managed by private or mixed companies where the state also has a significant share. That is why the

Government and the energy sector, in addition to their equally important and interconnected obligations, have legal responsibility for protecting the energy infrastructure of the Republic of North Macedonia as well.

In order to determine the key factors for adopting an effective strategy for protection of the energy infrastructure of the Republic of North Macedonia, in this section we will analyze the relevant legal and by-law acts that partially regulate the protection and security of energy infrastructure.

6.4. Legal Norms and Shortcomings for Adoption of Energy Infrastructure Protection Strategy of the Republic of North Macedonia

Appropriate strategic and legal solutions are a prerequisite for building an efficient system for critical infrastructure protection. Based on the examples of the majority of the EU and NATO Member States, in the search for the legal basis for protection of the energy infrastructure of the Republic of North Macedonia, the following should be analyzed:

- Defense Strategy of the Republic of North Macedonia;
- Law on Crisis Management;
- Law on Protection and Rescue;
- Law on Energy.

This approach is one of the possible ones, based on the assumption that each sector of critical infrastructure will have an appropriate strategic and legal solution that will enable efficient protection of critical infrastructure. As a result of the analysis, we will highlight several key findings that have been of great importance in terms of determining the legal shortcomings that the Republic of North Macedonia in the future will have to direct its efforts in the creation of favourable conditions for adopting a strategy for energy infrastructure protection.

6.4.1. Defence Strategy of the Republic of North Macedonia

Safety and protection of citizens is the primary responsibility of the Government of the Republic of North Macedonia. According to the Defence Strategy of the Republic of North Macedonia, "the development and maintenance of the security and defense system is one of the basic tasks of the Government of the Republic of North Macedonia in the interest of its citizens" (Defence Strategy of the Republic of North Macedonia, 2010). This obligation towards the national security of the Republic of North Macedonia cannot be fulfilled by the Government without adequate protection of energy infrastructure. The power sector, the oil and petroleum sector, as well as the other segments of the energy infrastructure are an integral part of the security and well-being of North Macedonian citizens. Similarly, to the state, citizens of the Republic of North Macedonia need a functional and stable energy infrastructure – resistant to asymmetric threats, natural or technological disasters – which will timely and in the required quantities supply the energy resources necessary for maintaining and advancing the security and well-being of Macedonian citizens.

Therefore, in addition to the state authorities, companies, public enterprises, institutions, services and units of local self-government, can perform special tasks in the area of defense, especially in the function of energy infrastructure security. This is especially true for energy operators, which, driven by the goal of safe, timely, and quality supply of consumers – including citizens and state authorities – are obliged to undertake appropriate preventive and safety measures covered by other legal and by-law acts analyzed in this section. In order to be able to respond to the complex requirements arising from strategic commitments for full integration into the EU and NATO, the defense system of the Republic of North Macedonia is being built and developed based on several factors, which indirectly affect the national energy infrastructure. Assessment of contemporary security threats, risks and challenges at national, regional and global level, geopolitical determinants, as well as national resources and projected economic opportunities of the state are the key factors that should be taken into account in the planning, organization and realization of protection of the national energy, i.e. critical infrastructure. As one of the pillars of the defense system, the Strategy emphasizes the development of the operational capabilities of the Army of the Republic of Macedonia, in two directions related to the security of energy infrastructure. The first is the support of the police and other state institutions in critical infrastructure protection and support in dealing with the consequences in the event of a terrorist attack, while the second is the support of state institutions in case of natural disasters and epidemics, technical and technological and other dangerous and crisis conditions/ situations (Chaminski, 2017: 168).

6.4.2. Law on Crisis Management

The leading role of the Government in the process of protecting the critical, i.e. energy, infrastructure is also defined in the Law on Crisis Management that regulates the crisis management system in the Republic of North Macedonia (Law on Crisis Management, 2005). In addition to the Government and other state administration bodies and state authorities, the ARM and the protection and rescue forces, public enterprises, public institutions and services, as well as trade companies, can participate in prevention, early warning and dealing with crises. They have an obligation to protect and save the employees, the persons on spot and the material goods, as well as remove the consequences of the crisis situation. Although there is no explicit emphasis on the term, however – when it comes to energy operators – it is understood that "material goods" represent the energy infrastructure they manage. In addition, the ministries and other state administration bodies and municipalities, public institutions and services, as well as companies of special importance for operating in crisis situations, have an obligation in their acts for organization and systematization to establish jobs for the preparation and execution of working tasks related to prevention and rescue in a crisis situation. According to Article 12 of the Law, a Steering Committee, an Assessment Group and a Directorate / Centre for Crisis Management are established within the crisis management system. In addition to the measures and activities undertaken by the Steering Committee in a crisis situation, it has an obligation to provide timely, high-quality and realistic assessment of the threat to the security of the Republic

from the risks and dangers. Given the fact that it is composed of the ministers of interior, health, transport and communications, defense and foreign affairs, then it can be undoubtedly concluded that the government's leadership in the critical infrastructure protection is not at all disputed. In addition to the Steering Committee, The Assessment Group is also a governmental body comprised of the Directors of Public Security Bureau, the Security and Counterintelligence Administration, the Intelligence Agency, the Directors and Deputies of the Directors of the Crisis Management Centre, and the Directorate for Protection and Rescue, the Deputy Chief of General Staff of the ARM and the Head of Security and Intelligence Service in the Ministry of Defence. As a body whose leader is appointed by the Government of the Republic of North Macedonia, the Assessment Group has a permanent task – not only in case of a crisis – to assess the risks and dangers to the country's security, and to propose measures and activities for their prevention, early warning and in the end to deal with the crisis situation. The Assessment Group submits the results and conclusions to the Steering Committee, the President of the Government, the President of the Republic and the President of the Assembly. The Crisis Management Center is an independent authority and holder of the overall support of the Steering Committee, and the Assessment Group that provides continuity in the inter-ministerial and international cooperation in crisis management, prepares and updates a unique assessment of the risks and dangers for the security of the Republic of North Macedonia. As an operational expert body, which manages the activities for prevention and dealing with crisis situations, a Headquarter is formed within the Centre, consisting of representatives of the bodies involved in the work of the Steering Committee. Based on the foregoing, it can be concluded that the Law delegates the responsibility to each of the institutions involved in the organs and bodies in the crisis management system to undertake measures and activities for collecting information and identifying security risks and dangers, including those which endanger the security of energy infrastructure. Within the legal framework and authorizations, the institutions covered by the crisis management system, based on their assessments, determine the objectives, tasks and implementation of the necessary actions for prevention, early warning and crisis management. Among other things, the participants in the crisis management system are obliged to mutually communicate, coordinate and cooperate with the Centre upon the performance of the duties determined by the Law. For the purpose of planned, timely, expedient and coordinated decision-making, directions and recommendations for undertaking measures for prevention, as well as for the most optimal handling of the crisis situation, an assessment is made of the threat to the security of the Republic of North Macedonia from all the risks and dangers, that is adopted by the Government. As for the implementation, that is, the implementation of the provisions of this Law, the Crisis Management Centre prescribes inspection supervision in the state administration bodies, municipalities and other elements of the public and private sector and provides for appropriate penal provisions in the event of non-compliance with the decisions and other measures prescribed by the Law on Crisis Management. (Chaminski, 2017: 168-171)

6.4.3. Law on Protection and Rescue

Protection and rescue, is a matter of public interest for the Republic of North Macedonia and is organized and carried out not only by state and administrative bodies, but also by all public institutions, trade companies, including energy operators. According to the relevant Law, the protection and rescue system is realized through a number of measures and activities, including: observation, detection, monitoring and study of the possible dangers of natural disasters and other accidents; undertaking preventive measures, reporting and warning; determining and implementing protective measures; supervision of the implementation of protection and rescue; identification and assessment of hazards; preparation of the assessment of threats from natural disasters and other accidents and plans for protection and rescue and updating thereof, etc. In addition to the natural disasters, the stated measures and activities are also undertaken for assessment and prevention of other accidents. The Law defines them as events that result from certain overlooks and errors in the execution of everyday economic and other activities, as well as carelessness in the handling of dangerous goods and means for production, storage and transport of such goods (fires, major accidents in road, rail and air traffic, mine accidents, industrial accidents caused by explosions and other technical and technological reasons, radioactive rains, dust and sludge, spills of oil and oil derivatives and other toxic chemicals, explosion of gases, flammable liquids and gases and other flammable substances which create explosive mixtures with the air and other explosive materials of a larger size). Although asymmetric threats are not explicitly listed in the Law, nevertheless there is a high likelihood of "deliberate overlook of mistakes" (sabotage or diversion) in the handling of the listed dangerous goods, some of which are primary or final products of the energy sector of the Republic of North Macedonia. The following eight principles on which the protection and rescue in the Republic of North Macedonia is based, in terms of energy infrastructure, are the most significant: everyone has the right to protection and rescue from natural disasters and other accidents; the Republic of North Macedonia, municipalities, public enterprises, institutions and services and trade companies are obliged to timely organize and undertake preventive and operational measures for protection and rescue from natural disasters and other accidents; any natural and legal person, in accordance with the Law, is responsible for failure to implement the foreseen protection and rescue measures, etc. Of particular importance for the protection of energy infrastructure is the principle that obligates the security system institutions, and the public and private sector companies (including the energy operators) to organize and undertake, above all operational measures, to which the strategies for critical infrastructure protection of modern democratic states have a key role in the process of achieving the goals of the respective national strategies. The planning of the protection and rescue is realized on the basis of the National Strategy for Protection and Rescue adopted by the Assembly upon proposal of the Government of the Republic of North Macedonia. In view of organized implementation of the protection and rescue, all participants in the system adopt a Plan for protection and rescue from natural and other disasters. The Protection and Rescue Plan is prepared on the basis of the assessment of threat of natural and other disasters on the territory of the Republic

of North Macedonia, while for the needs of the private sector, including the energy operators, the assessment is adopted by the managing body. Accordingly, it can be concluded that the assessment of the endangerment of privately owned energy providers – according to the available information – is adopted by the management, on the basis of which is adopted the protection and rescue plan after which it undertakes the further measures and activities for securing the infrastructure from natural disasters and other threats (Law on Protection and Rescue, 2012).

6.4.4. Law on Energy

The Law on Energy is another legal act that coincides with the primary responsibility of the Government of the Republic of North Macedonia - security and protection of its citizens. Reliable, safe and quality supply of consumers with energy and fuels, creation of an efficient, competitive and financially sustainable energy sector, and protection of the environment from negative impacts in the performance of certain activities in the field of energy, are part of the main goals of this law (Law on Energy, 2018).

The Law on Energy is the only law that covers the concepts: security, protection, energy (fuel types) and infrastructure. Under the term "security", the Law on Energy defines the ability to ensure the protection of the health and life of people, protecting the environment and property by undertaking technical and other types of safety measures in the production, transmission and distribution of energy or fuels. In addition to the various types of fuels, the Law defines most of the components of the energy infrastructure, such as gas pipeline, oil pipeline, distribution network for electricity, power system, energy facility, energy sector, operator, electricity producer, etc. In addition, the Law regulates numerous rights and obligations that energy operators should undertake in order to protect the energy infrastructure and security of supply not only to citizens, but also to the institutions of the national security system. According to the Law on Crisis Management, the operators of the transmission and distribution systems of the appropriate type of energy or fuel are obliged to prepare operation plans for crisis situations and submit them for approval to the Ministry of Economy. Furthermore, distribution system operators are obliged to adopt and publish distribution rules which, inter alia, regulate: the technical and other requirements for the safe and secure operation of distribution systems; measures, activities and procedures in case of disturbances and major accidents; prescribed safety measures and so on. Furthermore, the Law provides for strict security measures that potential investors in the energy sector must undertake as a prerequisite for obtaining authorization for the construction of energy facilities. These measures relate to the safety and security of the energy system, facilities and appropriate equipment, public health protection and safety, and environmental protection. Although there are adequate legal bases and obligations for protection of the energy, i.e. critical infrastructure in which the central government plays the key role, the Republic of North Macedonia significantly lags behind the type and effectiveness of the legal regulations for critical infrastructure protection of the EU and NATO Member States, as analyzed in the previous chapter. As a candidate country for full-fledged membership

in the EU, the Republic of North Macedonia should follow the steps that the Union and its members undertake in order to protect the critical infrastructure. Therefore, the Government of the Republic of North Macedonia must first define the critical infrastructure, and then proceed with preparation and adoption of a Program for the Protection of National Critical Infrastructure as a basis for the development of an effective strategy for its protection. The Program should be the result of a constructive cooperation that must be established and maintained between the private sector – including energy operators – and the competent governmental institutions at the state and local levels, not only in crisis but also in peaceful conditions. The main goal of this cooperation is to create an operational and effective national framework for joint action and build elastic and stable critical infrastructure, following the example of the organization of organs and bodies in the crisis management system. The preparation of a draft strategy for critical infrastructure protection, involving competent governmental institutions, operators and private sector companies, as well as experienced experts in the area of official infrastructure security, is the next step in the process of adopting an effective strategy for protection of energy, i.e. critical infrastructure. The purpose of the draft strategy is to develop and define a centralized, integrated and progressive strategy that will involve voluntary participation of industrial, energy and other private sector operators, as well as competent institutions from the central and local government. The desired outcome of the strategy is sufficiently elastic and immune – on security risks and threats – critical infrastructure that will enable citizens to have continuous and guaranteed access to basic services, including the supply of the necessary energy resources. One of the guiding principles of the strategy is raising awareness among energy and industrial operators and central and local governments of the need to protect the national critical infrastructure, as well as the need for full and permanent integration of intelligence and security assessment into crisis management plans.

If a comparison is made between the Crisis Management Law, the Law on Protection and Rescue and the Energy Law, it can be concluded that public enterprises, trade companies, industrial facilities and energy operators, can voluntarily and contractually participate in prevention, early warning and dealing with natural and security risks and hazards. However, without an operational framework for cooperation, the institutions of the national security system and the management of energy operators are unable to effectively implement and coordinate the measures and activities for protection of the energy infrastructure. Addressing this problem should not be perceived solely as a national problem, but it is an obligation that the state has as an aspirant for full membership in the EU and NATO. Energy operators must have sufficient information necessary for relevant security assessment on the basis that will plan and implement the necessary measures for infrastructure protection. This applies in particular to asymmetric threats for which energy operators have neither capacity nor legal powers to collect intelligence of such character. Therefore, the creation of a common integrated approach in the function of energy infrastructure security should be equally important and legal imperative, both for the Government and the energy operators. (Chaminski, 2017: 172-175).

6.5. Elements and Model of a Strategy for Energy Infrastructure Protection

The modern concept of energy infrastructure protection, as an integral part of national strategies for critical infrastructure protection, consists of a series of consecutive and interconnected elements that regulate the security of the energy sector as the main instigator of the economic and development policies of modern democratic states. Today, almost all parts of the private and public sector depends on the infrastructure that provides the necessary energy resources for its smooth and safe operation. Therefore, the focus of critical infrastructure protection is precisely the energy facilities that are necessary for the functioning of the political, social, economic and security processes in the society. In planning the elements of the Strategy for Energy Infrastructure Protection, whether it will be an independent or integral part of the Strategy for Critical Infrastructure Protection, it should be taken into account that every segment of the energy sector in the Republic of North Macedonia consists of a complex physical, computer, institutional, functional and personal structure whose functioning is impossible without the use of modern communication systems and the Internet. Most of the facilities for electricity generation, transmission and distribution are on the surface of the earth and are visible. Excluding rail and road transport, as well as control towers, the infrastructure for transmission and distribution of natural gas and oil is located below the surface of the earth and (with certain exceptions) it is not visible but is marked. Therefore, a unique methodology for identifying energy objects, systems and functions that have critical significance for the state and priority in terms of their protection should be developed. For that purpose, it is necessary to create a comprehensive, spatial and temporary updated database for precise determination of critical facilities, systems and functions, as well as a specific division of responsibilities between the private and the state sector. The risk of an attack on the energy infrastructure varies with the value and importance of the capacity (production, processing, storage, transport – oil pipeline, gas pipeline, transmission line – distribution, etc.). In the recent years, energy infrastructure has become a legitimate goal for global terrorist organizations as well. The accelerated process of globalization and the inevitable international trade in energy resources has further increased the risk of terrorist attacks on energy infrastructure. Although the Republic of North Macedonia and the wider SEE region have not faced direct terrorist attacks, however, the attack and disabling of the energy infrastructure of the countries where they originate or through which the energy resources transit can have a serious impact on the national energy security and economic development of the country. In addition to financing their own activities, terrorist organizations are trying to cause serious damage to the energy infrastructure with armed or cyber-attacks from a distance in order to create panic in the society, halt industrial production and, above all, stop the transmission of electricity, oil and oil derivatives. In terms of threats, the various elements of the energy infrastructure of the Republic of North Macedonia are characterized by varying degrees of vulnerability. The threat to security of certain energy facilities can result in a serious ecological disaster, although they are located in a relatively small area that physically can be easily secured. The oil and petroleum production sector, as

well as the natural gas sector, is characterized by a spatial infrastructure whose damage can lead to a disruption of the supply, exhaustion of state reserves and reduction of economic and defense capabilities. The situation is similar with the power sector whose main weakness pose its centralized automatic management and the lack of capacities for accumulation of necessary quantities of electricity. Considering the fact that the energy infrastructure has a great importance for the economic and security situation of the Republic of North Macedonia, its security is essential. In addition to terrorist threats, the energy infrastructure can be exposed to various types of threats that must be taken into account, both in the analysis and in assessment of risk and threats, as well as in defining security and preventive measures. These include natural disasters, technological accidents and human errors that can seriously compromise, cause major damage, or destroy certain sectors of the energy infrastructure of vital importance for the population and society as a whole. It can cause the so-called domino effect that has the potential to paralyze multiple sectors of critical infrastructure of the state, cause enormous damage to the national economy and loss of confidence in the political leadership of the state. In this context, the owners of the energy capacities and the institutions of the system, although they cannot fully guarantee the safety of the energy infrastructure, in accordance with the legal regulations of the Republic of North Macedonia, they are obliged to take appropriate and timely measures to reduce the risk of damage to the infrastructure and re-establish the supply of the necessary energy resources under favourable conditions.

Since the security of energy infrastructure is a common task of the government and the energy operators at the national and local level, their efforts should be directed towards raising the level of its protection on the territory of the state by undertaking appropriate and mutually coordinated measures. After identifying critical parts of energy infrastructure and assessing risk and threats, prevention is the fundamental measure in the function of protecting energy infrastructure. In case of damage, an effective crisis management plan and preparedness of the energy operators are necessary for timely recuperation of the affected energy capacity in a functional state. To this end, according to the updated security assessments and experiences of the countries of the international community, it is necessary to develop – legally prescribed – standards for protection that will provide a sustainable energy infrastructure, immune to modern security threats. The consistent application of preventive measures, the standards for protection and their proper management in the form of a crisis management cycle for the energy infrastructure, represent the basic guarantee for effective protection of the energy infrastructure of the Republic of North Macedonia. The biggest requirement that must be fulfilled for achieving the stated strategic goals is the need for continuous exchange of information and cooperation between government institutions and energy operators. Without this condition, the implementation of the strategy for energy infrastructure protection cannot be expected in real terms, since it includes a set of plans, programs, measures and instruments for coordination and promotion thereof, both by governmental institutions and energy operators.

Based on the findings obtained from the comparative analysis of the strategies for critical infrastructure protection of some of the EU and NATO Member States

and the current legislation for energy infrastructure protection of the Republic of North Macedonia, one can conclude that the model of the National Strategy for Energy Infrastructure Protection – individually or as part of a national critical infrastructure – represents a whole composed of the following interconnected and dependent elements:

- Strategic goals and interests of the state in relation to energy infrastructure, defined in the National Security Strategy;
- Harmonized legislation;
- Defining main elements of critical / energy infrastructure and sharing responsibility;
- Assessment of security threats, risks and vulnerability of elements of energy infrastructure;
- Determine the strategic goal of the strategy – effective protection of the critical / energy infrastructure;
- Cooperation, coordination and exchange of information between the parties involved, and
- Implementation.

In addition to identifying the objectives of energy infrastructure protection, the proposed model sets out two levels of decision-making a political level and a level of special sectors of critical infrastructure.

The National Security Strategy and Critical Infrastructure Protection Strategy are articulated within the first level, while within the second level, the public and private sectors – jointly – create the specific objectives, measures and activities for the protection of sectors of critical infrastructure, including the energy sector as well. According to the proposed model, critical infrastructure protection objectives are set at the highest strategic level and are defined within the national security strategy. In addition to the objectives of protection, the comprehensive principles for critical infrastructure protection are defined at this stage. The next step is to create strategies for critical infrastructure protection that emphasize the specific sectors and sub-sectors of critical infrastructure, and the principles of protection (such as information exchange, private-public partnership, etc.) are implemented and further processed and concretized. This step leads to the process of transferring the strategy from a political, to the level of separate sectors. In other words, it comes to application of the objectives and principles for critical infrastructure protection – developed at a political level – are applied in the specific / separate sectors, where the public sector and private sector operators communicate and exchange information and experiences for the safety of sectors and sub-sectors from the identified critical infrastructure. In the level of separate sectors, the objectives and principles of protection are adapted to the specific needs of the identified and designated sector and sub-sector of critical infrastructure. This results in the creation of plans to protect each sector of critical infrastructure, including the energy sector. At this stage, the role of energy or industrial operators in the private sector is to manage sectors of critical infrastructure, co-operate with

the public sector, and articulate goals and measures to achieve the required level of infrastructure protection. Within the public sector, dedicated agencies (such as the Crisis Management Centre, the Protection and Rescue Directorate, etc) share the national legal obligations to critical infrastructure operators and create platforms for the exchange of information and partnerships.

In addition to the described critical infrastructure protection model, which is based on the traditional "top-down" approach, there is a "bottom-up" approach that using feedback information, informs the political level of the effectiveness of objectives, principles and measures for protecting sectors of critical infrastructure. At both levels, the wider information provides insights and influence on the identified goals, principles, measures and means for critical infrastructure protection sector, both by the public sector institutions and by the national / local agencies as well as by the operators of the private sector and academic community. Accordingly, it can be concluded that the proposed Draft Model is an example of a dynamic, interactive, and, above all, an effective process involving all parties that play a role in the process of defining, promoting and implementing goals, principles and measures for energy infrastructure protection as a key sector of the critical infrastructure of the Republic of North Macedonia. (Chaminski, 2017: 175-181).

Conclusions and Recommendations

As we have already mentioned, critical infrastructure is a platform for maintaining the development of every society and state. Hence, the Government should be involved in the critical infrastructure protection system as a legislator that brings laws and by-laws and has the task of authorizing certain ministries to be coordinators of the entire system.

The Government provides a strategic framework that is essential for the successful functioning of the system, cooperation, communication and coordination of all involved actors. The Government also determines (by special decision) sectors of certain critical infrastructures in order to provide a holistic approach to protecting and reducing adverse impacts in case of a threat to critical infrastructure.

After the Government, the next most important actor is the coordinator (designated ministry) of the entire system for critical infrastructure protection. There are various examples and practices on which body is appropriate for this role. In many European countries, this function has been assigned to the Ministry of the Interior. Hence, there are different solutions and practices, but each country should recognize the most appropriate model on its own. From a comprehensive analysis, we propose that the Ministry of Interior of the Republic of North Macedonia be the coordinator of the whole system for critical infrastructure protection.

If the Ministry of the Interior is a system coordinator, it will have the role to communicate directly with all actors of the system, with international actors and submit reports to the Government.

An organizational approach to the implementation of critical infrastructure protection in the European Union and countries that strive towards full membership

(such as the Republic of North Macedonia) is given in Directive 2008/114/EC on the identification and establishment of European critical infrastructures and the assessment of the need to improve their protection – the main document of the European Union for critical infrastructure.

In order to be resolutely committed to the implementation of the above, we provide several initial recommendations:

1. In the establishment of the critical infrastructure protection system, it is necessary to have the strategic framework as a starting point. It is necessary to incorporate the strengthening of the resistance and the critical infrastructure protection into one of the Strategies of the Republic of North Macedonia. There are several possibilities:
   A. *If the need for revision of the existing or development of a new national security strategy is to be established, it is necessary to include a section for critical infrastructure in the strategy. It is indisputable that the National Security Strategy should include a section on critical infrastructure.*
   B. *If there exists or is in the development of a Cyber Security Strategy, the critical infrastructure can be mentioned there. Such a Strategy was developed in 2018 and contains sections that aim to protect the critical information infrastructure as part of the overall critical infrastructure. Furthermore, an action plan for protection of critical information infrastructure has also been adopted.* (National Strategy for Cyber Security of the Republic of Macedonia, 2018-2022).
   C. *The third solution is a proposal for the preparation of a Strategy for Critical Infrastructure Protection.*
2. Normatively, the drafting of the Law on Critical Infrastructure Protection can be proposed. While it does not pass all the foreseen phases of its adoption, the critical infrastructure topic may be temporarily regulated under any other law or by-law (the assumption is that the procedures for this are shorter and faster can be temporarily regulated).
3. When drafting the normative regulation for critical infrastructure, the recommendation is to regulate primarily the areas of energy and transport – these two segments are required by the European Union from its Member States and those that aspire to access the Union. If other critical infrastructure sectors are involved, the experience of Croatia can be repeated at the very beginning to slow down and complicate the process. Therefore, it is recommended to start with the energy and transport sectors.
4. In the forthcoming normative solutions (law and by-laws), the possibilities for regulation of the European critical infrastructure should be foreseen.
5. In the law and by-laws, the security coordinator must be mentioned, which is a key figure that will be responsible in all bodies and organs for the activities regarding the critical infrastructure.
6. In the law or by-laws, to emphasize the place and role of the public-private partnership.
7. In the law or by-laws, to emphasize education, and training.

8. The place and role of the newly established Critical Infrastructure Protection Centre is extremely important. For these reasons, perhaps the Ministry of the Interior is a good choice to be a state coordinating body for this process, because the Centre should collect data and coordinate activities. Also in the law or by-laws, it is important to state that the work on critical infrastructure protection will take place through the Centre for Critical Infrastructure Protection.
9. As far as the classification is concerned, the lowest possible classification should be put in place so that we do not get into the situation to block the process from the very beginning.
10. In creating the strategic solutions and the legal solution, an inter-ministerial group should be established that will include a wider circle of experts, from universities, ministries, chambers, the private sector.
11. After the adoption of the law, further by-laws should regulate individual procedures.

After the Strategy and the Law, it is necessary to begin the establishment of the Critical Infrastructure Protection SYSTEM. The SYSTEM is built by education, workshops and familiarization of all stakeholders in that process. It is necessary to make a five-year action plan.

Literature

[1] Alcheski, Gj., (2016), Implementacija na sovremenite bezbednosni sistemi i proceduri vo razvojot na obezbeduvanjeto na obukite od vitalen interes za Republika Makedonija (so osvrt na aerodromskata bezbednost), Filozofski fakultet, Skopje;

[2] Amin, M. (2000), National Infrastructures as Complex Interactive Networks, in: Samad, T. i Weyrauch, J. (ed.) Automation, Control, and Complexity: An Integrated Approach, New York: John Wiley and Sons, pp. 263-286;

[3] Amin, M. (2002), Modeling and Control of Complex Interactive Networks, IEEE Control Systems magazine http://massoud-amin.umn.edu/publications/Amin_IEEE_CSM_Feb_02.pdf;

[4] Antoliš, K. (2013), *Intellectual Capital and National Critical Infrastructure*, New security threats and national critical infrastructure. Zagreb: Ministry of the Interior of the Republic of Croatia, Police Academy, pages 7-14;

[5] Babos T. (2016) *The First Critical Infrastructure Protection Research Project in Hungary*. In: L. Nádai and J. Padányi (eds.), Critical Infrastructure Protection Research, Topics in Intelligent Engineering and Informatics 12, Springer International Publishing Switzerland;

[6] Bell, G.R., (2009) NATO's Grapple with Energy Security. In: Luft, G., Korin, A. (eds.) (2009) Energy Security Challenges for the 21st Century: a Reference Handbook. Santa Barbara: ABC-CLIO;

[7] Benjamin K. Sovacool (2010) *A Critical Evaluation of Nuclear Power and Renewable Electricity in Asia,* http://dx.doi.org/10.1080/00472331003798350;

[1] Bognar, B. 2009. The process of critical infrastructure protection, AARMS, Budapest;

[2] Braubach, A., Lauwe, P. and John-Koch, M. (2014), *CIP in Germany: Cooperation and recommendations as main driving forces,* Global Security 2014, pg. 5-14;

[3] Brian Wilson, (2012), Maritime Energy Security. NATO Centre of Excellence Defence Against Terrorism (COEDAT) in November 2012;

[4] Butorac, K. (2013), Risk Assessment Methodologies in Critical Infrastructure Protection, New security threats and national critical infrastructure. Zagreb: Ministry of the Interior of the Republic of Croatia, Police Academy, pages 46-58;

[5] Čemerin, D. (2013), Croatian Critical Infrastructure, Opatija: Fifth Adriatic City Security Conference, http://zastita.info/hr/sigg_2013/program0/;

[6] Cesarec, I. (2017), An overview of former and present activities of regulating Critical Infrastructure System in the Republic of Croatia, Opatija: Ninth Adriatic City Security Conferencehttp://www.zastita.info/UserFiles/file/zastita/SIGG/SIGG%202017/Prezentacije/06.%20Ivana%20Cesarec.pdf;

[7] Cesarec, I. (2019), The Civil Protection Directorate of the Republic Croatia, National Contact Point for Critical Infrastructure (electronic correspondence of authors);

[8] Chaminski, B., (2017) Geopolitichko znachenye i zashtita na energetskata infrastruktura na Republika Makedonija od asimetrichni zakani. Doktorska disertatsiya. March, 2017;

[9] Dawson M., Omar M., 2015. NewThreats and Countermeasures in Digital Crime and Cyber Terrorism Information Science Reference;

[10] Deutscher Bundestag (2015), *Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)* http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf (Accessed August 14 2017.);

[11] Ducamin, I. 2016. State and Operators Cooperations for Critical Infrastructure Protection;Buliding Trust for Common Interest;

[12] Engdahl, E-M. (2016), *The European Programme for Critical Infrastructure Protection,* Gas Infrastructure Europe, http://www.gie.eu/index.php/publications/doc_download/26303-critical-infrastructure-protection-in-europe;

[13] Ericsson (2019), Future mobile data usage and traffic growth, https://www.ericsson.com/en/mobility-report/future-mobile-data-usage-and-traffic-growth;

[14] Ford, N. (2015), *New German cyber security law to protect critical infrastructure,* IT Governance Ltd, https://www.itgovernance.eu/blog/en/new-german-cyber-security-law-to-protect-critical-infrastructure/;

[15] Haemmerli, B. and Renda, A. (2010), *Protecting Critical Infrastructure in the EU,* Brussels: Centre for European Policy Studies, https://www.ceps.eu/system/files/book/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf;

[16] Johansson, J. (2010), *Risk and Vulnerability Analysis of Interdependent Technical Infrastructure: Addressing Socio-Technical Systems,* Lund University, Sweden;

[17] John-Koch, M. (2017), Head of Division II.3 – Critical Infrastructure Protection (CIP) Strategy, Cyber Security CIP, Federal Ministry of the Interior of the Republic of Germany (electronic correspondence of authors);

[18] Kandek, W. (2015.), Germany's approach to securing critical infrastructure - a benchmark for others?, SC Magazine, https://www.scmagazineuk.com/germanys-approach-to-securing-critical-infrastructure--a-benchmark-for-others/article/534852/;

[19] Keković, Z. 2013. National Critical Infrastructure protection regional perspective, Belgrade;

[20] Lars K. Kristian (2015) Unfolding Green Defense. Linking green technologies and strategies to current security challenges in NATO and the NATO member states. Copenhage: CENTER FOR MILITÆRE STUDIER KØBENHAVNS UNIVERSITET;

[21] Lazari, A. (2014) European Critical Infrastructure Protection. Springer International Publishing, Switzerland;

[22] Lazari, A. (2014), *European Critical Infrastructure Protection,* Springer International Publishing Switzerland;

[23] Lazari, A. and Simoncini, M. (2014), *Beyond compliance: An analysis of the experiences that maximise the implementation of the Directive 114/08/EC on European Critical Infrastructures,*International Juornal of Critical Infrastructure, https://www.dropbox.com/s/gvs5jhivvhqd3on/IJCIP-S-14-00008.pdf;

[24] Levis, G., 2006. Critical Infrastructure in Homelend Security-Defending a Net-worked National, John Wiley&Sons Inc.Hoboken, New Jersey (USA);

[25] Lopez, J., Setola, R. and Wolthusen, S. D. (2012), Overview of Critical Information Infrastructure Protection, LNCS 7130, pp. 1-14, Springer-Verlag Berlin Heidelberg;

[26] Malnar, D. and Mlinac, N. (2014), *Security-Intelligence Component for the Protection of the Critical National Energy Infrastructure of the Republic of Croatia,* University of Applied Sciences Velika Gorica: Book of Proceedings of the Seventh International Conference "Crisis Management Days", page 1007-1020, http://dku.hr/wp-content/uploads/2016/09/DKU-zbornik-radova-2014.pdf;

[27] Mark r. Chhasin and Jerod m. Loeb. High-Reliability Health CareL Getting There fromHere. TheMilbank Quarterly, Vol.91, No.3, 2013, p.459-491;

[28] Mikac R., Cesarec I.&Larkin R. 2018. Kritična infrastruktura-platforma uspješnog razvoja sigurnosti nacija. Naklada Jesenski I Turk, Zagreb;

[29] Mikac, R. (2017), *What's more, and the less important?,* Zagreb: Zaštita Journal, Number 3;

[30] Mikac, R. and Cesarec, I. (2016), *Critical Infrastructure Security and Resilience of the Republic of Croatia*, The CIP Report International Issue, August 2016, Washington: George Mason University – Center for Infrastructure Protection & Homeland Security, https://cip.gmu.edu/2016/08/18/critical-infrastructure-security-resilience-republic-croatia/;

[31] Mikac, R. and Cesarec, I. (2019), *Current state of play of the Republic of Croatia regarding Critical infrastructure security and resilience*, accepted publication work as a chapter in a book to be published by Springer International;

[32] Mileski, T., (2014) Energetska bezbednost. Skopje: Filozofski fakultet;

[33] Mitrevska M., Mikac R., 2017: Handbook on Critical Infrastructure protection, Chamber of Republic of Macedonia for Private security, Skopje, Macedonia;

[34] Monaghan, A. (2008) Energy Security: NATO's Limited, Complementary Role;

[35] Moteff J., Parfomak P., 2004. Critical infrastructure and Key Assetc: Definition and Identification, Congressional Research Service, the Library of Congress;

[36] O'Rourke, T. D. (2007), Critical infrastructure, interdependencies, and resilience, BRIDGE-Washington-National Academy of Engineering, 37(1), pp. 21-29, https://pdfs.semanticscholar.org/6c17/b35ec7555a9f27d5ccb6ca1d357a20b5ce0a.pdf;

[37] Perešin, A. and Klaić, A. (2012), The role of cyber security in critical infrastructure protection, University of Applied Sciences Velika Gorica: Book of Proceedings of the Fifth International Conference "Crisis Management Days", page 335-355, http://dku.hr/wp-content/uploads/2016/09/zbornik2012.pdf;

[38] Pokaz, I. (2013), The importance of intelligence support to critical infrastructure owners / managers, New security threats and national critical infrastructure. Zagreb: Ministry of the Interior of the Republic of Croatia, Police Academy, pages 279-289;

[39] Pokaz, I. and Perčić, U. (2014), Critical Infrastructure and Crisis Management, University of Applied Sciences, Book of Proceedings of the Seventh International Conference "Crisis Management Days", pages 1129-1144, http://dku.hr/wp-content/uploads/2016/09/DKU-zbornik-radova-2014.pdf;

[40] Popovski V;, 2019. Contemporary Macedonian Defence, Ministry of defence Republic of Macedonia, No.36/2019, p.61;

[41] Poustourli, Aikaterini & Kourti, Naouma. (2014). STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION (CIP) -THE CONTRIBUTION OF ERNCIP. https://www.researchgate.net/publication/304777853_STANDARDS_FOR_CRITICAL_INFRASTRUCTURE_PROTECTION_CIP_-THE_CONTRIBUTION_OF_ERNCIP (пристапено на 17.06.2019);

[42] Radoman, J. Securitization of Energy as a Prelude to Energy Security Dilemma. Western Balkans Observer, Issue: 4/2007;

[43] Roberts, K.H., 1990. Some characteristics of highreliability organizations. Organization Science, 1, 160-177;

[44] Santillan, M. (2015), Germany Introduces New Law to Strengthen Critical Infrastructure Protection, Tripwire, https://www.tripwire.com/state-of-security/latest-security-news/germany-introduces-new-law-to-strengthen-critical-infrastructure-protection/;

[45] Setola, R., Luiijf, E. and Theoharidou, M. (2016), Critical Infrastructures, Protection and Resilience, pp. 1-18, in: Managing the Complexity of Critical Infrastructures - A Modelling and Simulation Approach, Springer Open;

[46] Thomas Noonnan and Edmund Archuleta (2008) The Insider Threat to Critical Infrastructures, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf;

[47] Varwick, J. (2008) NATO's Role in Energy Security. NATO at a Crossroads. IP Summer 2008;

[48] Weick, K.E. 1990. The vulnerable system:An analysis of the Tenerife airdisaster. Journal of Management, 16/3, p.571-593;

[49] Zamorano, J. and Franco, A. (2019), Drought hits Panama Canal shipping, highlights climate fears, The Washington Post, 30 April 2019, https://www.washingtonpost.com/business/drought-hits-panama-canal-shipping-highlights-climate-fears/2019/04/30/f8dc5be0-6afc-11e9-bbe7-1c798fb80536_story.html?utm_term=.95741bb41126.

REPORTS AND DIRECTIVES

[1] Association of Old Crows, CACI International Inc, and the Center for Security Policy (2014), *Countering Asymmetric Threats: Cyber, Electronic Warfare and Critical Infrastructure*, Asymmetric Threat Symposium Eight, https://www.asymmetricthreat.net/pdf/symposium8_report.pdf;

[2] Aviation Law, "Official Gazette of the Republic of Macedonia", Skopje, no.63/2015;

[3] Brookings Doha Center Analysis (2016) *Risky Routes: Energy Transit in the Middle East*, https://www.brookings.edu/wp-content/uploads/2016/07/en-energy-transit-security-mills-2.pdf;

[4] Brussels Summit Declaration. 11 July 2018. www.nato.int;

[5] Bucharest Summit Declaration, NATO Press Release (2008/049) 3 April 2008. www.nato.int;

[6] Cabinet Office of the *Government of the United Kingdom* (2008), *The National Security Strategy of the United Kingdom*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf;

[7] Cabinet Office of the *Government of the United Kingdom* (2008), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61934/national_risk_register.pdf;

[8] Cabinet Office of the *Government of the United Kingdom* (2009), *The National Security Strategy of the United Kingdom*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229001/7590.pdf;

[9] Cabinet Office of the *Government of the United Kingdom* (2010), *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf;

[10] Cabinet Office of the *Government of the United Kingdom* (2010), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211853/nationalriskregister-2010.pdf;

[11] Cabinet Office of the *Government of the United Kingdom* (2012), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211858/CO_NationalRiskRegister_2012_acc.pdf;

[12] Cabinet Office of the *Government of the United Kingdom* (2013), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf;

[13] Cabinet Office of the *Government of the United Kingdom* (2015), *National Security Strategy and Strategic Defence and Security Review 2015,* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf;

[14] Cabinet Office of the *Government of the United Kingdom* (2015), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf;

[15] Cabinet Office of the *Government of the United Kingdom* (2017), *The National Risk Register of Civil Emergencies,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf;

[16] Canadian Security Intelligence Service (2017) *Cybersecurity and Critical Infrastructure Protection*, https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php;

[17] Centre for the Protection of National Infrastructure (2017), *About CPNI*, https://www.cpni.gov.uk/about-cpni;

[18] Chicago Summit Declaration. 20 May, 2012. www.nato.int;

[19] Commitments in the field of Disaster Risk Reduction, http://www.osce.org/secretariat/123189;

[20] Communication from Commission to the Council and the European Parliament-Critical Infrastructure Protection in the fight against terrorism, 2004.

[21] Communication from the Commission on a European Programme for Critical Infrastructure Protection, 2006;

[22] Council of the European Union (2007), *The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*, EUR-Lex, Official Journal, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007D0124;

[23] 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*, Brussels, 2008/114/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:18:03:32008L0114:HR:PDF;

[24] Council of the European Union (2008), *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection***,** Brussels, 2008/114/EC, EUR-Lex, Official Journal, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF;

[25] Council of the European Union (2008), *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Brussels, 2008/114/EC, EUR-Lex, Official Journal, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF;

[26] 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*, Brussels,2008/114/EC,http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:18:03:32008L0114:HR:PDF;

[27] Croatian Parliament (2010), *Private Protection Act,* Official Gazette, number 68/2003, 31/2010, 139/2010, https://www.zakon.hr/z/291/Zakon-o-privatnoj-za%C5%A1titi;

[28] Croatian Parliament (2017a), *National Security Strategy of the Republic of Croatia,* Official Gazette, number 73/2017, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2017_07_73_1772.html ;

[29] Croatian Parliament (2017b), *Homeland Security System Act,* Official Gazette, number 108/2017, https://narodne-novine.nn.hr/clanci/sluzbeni/2017_11_108_2489.html;

[30] Croatian Parliament (2018), *The Cyber Security Act of the Key Service Operators and Digital Service Providers,* Official Gazette, number 64/2018, https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html;

[31] CTED Trends Reports (2017), https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-March-2017-Final.pdf (accessed on 03.05.2019);

[32] DCSINT Handbook, 2006, Critical infrastructure threats and terrorism, Kansas, No.1.02, p. 1;

[33] Defense Strategy of the Republic of Macedonia, "Official Gazette of the Republic of Macedonia", 30/2010. p.6 http://www.slvesnik.com.mk/Issues/2EDC3A5EF4DD1747A803A4D1FF418F11.pdf (accessed on 20.06.2019);

[34] Department of Defense (1998), *Critical Infrastructure Protection Plan*, https://fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm;

[35] Department of Homeland Security (2003), *Homeland Security Presidential Directive 7,* Washington, D.C., https://www.dhs.gov/homeland-security-presidential-directive-7#;

[36] Department of Homeland Security (2013), *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf;

[37] Department of Homeland Security (2015a), *Energy Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf;

[38] Department of Homeland Security (2015b), *Communications Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf;

[39] Department of Homeland Security (2015c), *Transportation Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf;

[40] Department of Homeland Security (2015d), *Water and wastewater Sector Specific Plan 2015,* Washington, D.C., https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf;

[41] Department of Homeland Security (2015e), Critical Infrastructure Cross Sector Council Charter, Washington, D.C., https://www.dhs.gov/sites/default/files/publications/cipac-cross-sector-council-charter-2015-508.pdf;

[42] Department of Homeland Security (2017a), *National Infrastructure Advisory Council, Future Focus Study: Strengthening the NIAC Study Process*, https://www.dhs.gov/sites/default/files/publications/niac-future-focus-study-strengthening-the-niac-study-process-final-508.PDF;

[43] Department of Homeland Security (2017b), *2017 National Preparedness Report,* Washington, D.C., https://www.fema.gov/media-library/assets/documents/134253;

[44] Department of Homeland Security (2019), *Homeland Security Presidential Directive 21,* https://www.dhs.gov/homeland-security-presidential-directive-21#;

[45] European Commission (2002), *Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection*, https://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf;

[46] European Commission (2004), *Communication on Critical Infrastructure Protection in the fight against terrorism,* EUR-Lex, Official Journal, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702;

[47] European Commission (2005), Green Paper on a European Programme for Critical Infrastructure Protection, EUR-Lex, Official Journal, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576;

[48] European Commission (2006), European Programme for Critical Infrastructure Protection, EUR-Lex, Official Journal, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786;

[49] European Commission (2013), *Commission staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure*, EUR-Lex, Official Journal, https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf;

[50] European Commission (2014) *ECHO Factsheet – Disaster RiskManagement – 2014,*http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/disaster_risk_management_en.pdf, p.1;

[51] European Commission (2014) The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience, http://ec.europa.eu/echo/files/news/post_hyogo_managing_risks_en.pdf;

[52] European Commission (2017), *Commission staff working document on assessment of the EU 2013 Cybersecurity Strategy*, EUR-Lex, Official Journal, http://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF;

[53] European Commission (2019), Cybersecurity, https://ec.europa.eu/digital-single-market/en/cyber-security;

[54] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013), *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, EUR-Lex, Official Journal, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf;

[55] European Environment Agency (2011) *Mapping the impacts of natural hazards and technological accidents in Europe* (Technical report No 13/2010), http://www.eea.europa.eu/publications/mapping-the-impacts-ofnatural/at_download/file;

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

[57] European Union Council Directive 2008, On the identification and designation of European Critical I nfrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, 23/12/2008;

[58] Federal Ministry of the Interior (2007), Critical Infrastructure Protection Implementation Plan, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation%20Plan.pdf?__blob=publicationFile;

[59] Federal Ministry of the Interior (2008), Protection of Critical Infrastructures Baseline Protection Concept, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/Baseline%20Protection%20Concept.pdf?__blob=publicationFile;

[60] Federal Ministry of the Interior (2009), National Strategy for Critical Infrastructure Protection, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile;

[61] Federal Ministry of the Interior (2011a), *Cyber Security Strategy for Germany,* Federal Republic of Germany, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/cyber%20security%20strategy.pdf?__blob=publicationFile;

[62] Federal Ministry of the Interior (2011b), *National Plan for Information Infrastructure Protection,* Federal Republic of Germany, http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf;

[63] Federal Ministry of the Interior (2016), *Cyber-Sicherheitsstrategie für Deutschland,* https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/2016_16_11_Cyber_Sicherheitsstrategie2016.pdf?__blob=publicationFile;

[64] FOCUS D5, 2012, Problem space report: Critical Infrastructure&Supply Chain Protection, Cross Border Research Association (CBRA);

[65] Government of the Republic of Croatia (2008), *National Strategy for the Prevention and Suppression of Terrorism,* Official Gazette, number 138/2008, https://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_139_3896.html;

[66] Government of the Republic of Croatia (2009) Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća;

[67] Government of the Republic of Croatia (2010), *Protection and Rescue Plan for the Republic of Croatia,* Official Gazette, number 96/2010, https://narodne-novine.nn.hr/clanci/sluzbeni/2010_08_96_2707.html;

[68] Government of the Republic of Croatia (2013a), *Critical Infrastructure Act,* Official Gazette, number 56/13, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html;

[69] Government of the Republic of Croatia (2013b), *Risk Assessment for Republic of Croatia from Natural and Technical – Technological Disasters and Major Accidents,* http://stari.duzs.hr/download.aspx?f=dokumenti/Clanci/PROCJENA_web_20.03.2013..pdf;

[70] Government of the Republic of Croatia (2013c), *The National Strategy and Action plan for the* Non-Proliferation of Weapons of Mass Destruction, https://vlada.gov.hr/UserDocsImages//Sjednice/Arhiva//71.%20-%206.pdf;

[71] Government of the Republic of Croatia (2013d), Decision on Designation the Sectors from which the Central State Administrative Bodies Identify National Critical Infrastructure and Lists of the Order of the Sectors of Critical Infrastructures, Official Gazette, number 108/2013, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_08_108_2411.html;

[72] Government of the Republic of Croatia (2014), *Statement from the closed part of the 140th session of the Government of the Republic of Croatia,* published on 6th February 2014, https://vlada.gov.hr/vijesti/priopcenje-sa-zatvorenog-dijela-140-sjednice-vlade-republike-hrvatske/14530;

[73] Government of the Republic of Croatia (2015a), *National Cyber Security Strategy,* Official Gazette, number 108/2015, https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html;

[74] Government of the Republic of Croatia (2015b), *National Strategy for the Prevention and Suppression of Terrorism,* Official Gazette, number 108/2015, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2015_10_108_2105.html;

[75] Green Paper on a European Programme for critical infrastructure protection, 2005, Brussels, Annex II;

[76] Home Office of the *Government of the United Kingdom* (2009), *National Counterterrorism Strategy*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf;

[77] Home Office of the Government of the United Kingdom (2011), The United Kingdom's Strategy for Countering Terrorism, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf;

[78] Joint Research Centre of the European Commission (2008), *Non-Binding Guidelines for application of the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection,* http://publications.jrc.ec.europa.eu/repository/bitstream/JRC48985/guidelines%20document%20final.pdf;

[79] Joint Research Centre of the European Commission (2017), *The ERNCIP Project Platform,* https://erncip-project.jrc.ec.europa.eu/;

[80] Law on Crisis Management, 2005. "Official Gazette of the Republic of Macedonia", 29/2005. http://www.macefdrr.gov.mk/files/dokumenti/pzrdo/Zakon%20za%20upravuvanje%20so%20krizi%202005.pdf (accessed on 21.06.2019);

[81] Law on Energy, 2018, "Official Gazette of the Republic of Macedonia", Skopje, no.96 from 28.5.2018 http://www.erc.org.mk/odluki/2%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%B7%D0%B0%20%D0%B5%D0%BD%D0%B5%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D0%BA%D0%B0_96_18.pdf (accessed on 21.06.2019);

[82] Law on Protection and Rescue, "Official Gazette of the Republic of Macedonia", 93/2012. http://www.slvesnik.com.mk/Issues/1F2D347B699C764F9E65C717889E74B2.pdf (accessed on 21.06.2019);

[83] Lisbon Summit Declaration. 20 November, 2010. www.nato.int;

[84] Military Doctrine of the Russian Federation. https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf (accessed on 10.06,2019);

[85] National Guidelines for Protection Critical infrastrukture from terrorism, 2011;

[86] National Institute of Standards and Technology (2018), *Framework for Improving Critical Infrastructure Cybersecurity,* Washington, D.C., https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf;

[87] National Protection and Rescue Directorate (2013), *Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure,* Official Gazette, number 128/2013, https://narodne-novine.nn.hr/clanci/sluzbeni/2013_10_128_2792.html;

[88] National Protection and Rescue Directorate (2016), *Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure*, Official Gazette, number 47/2016, https://narodne-novine.nn.hr/clanci/sluzbeni/2016_05_47_1221.html;

[89] National Protection and Rescue Directorate (2017), *Amendments to the Rules on the Methodology for Drafting Business Risk Analysis of Critical Infrastructure,* Official Gazette, number 93/2017, https://narodne-novine.nn.hr/clanci/sluzbeni/2017_09_93_2167.html;

[90] National Stategy for Cyber Security of the Republic of Macedonia 2018-2022. http://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf (accessed on 26.06.2019);

[91] National Strategy for Critical Infrastructure Protection (CIP Strategy) of Federal Republic of Germany, 2013;

[92] NATO ENSEC COE. https://enseccoe.org/en/ (accessed on 10.06.2019);

[93] NRDC.org (2018), *Flint Water Crisis: Everything You Need to Know*, https://www.nrdc.org/stories/flint-water-crisis-everything-you-need-know;\

[94] Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastructure državnega pomena v Republiki Sloveniji, 2012: 1-2-3;

[95] Patriot Act, 2001.

[96] Prague Summit Declaration (2002); https://www.nato.int/cps/en/natohq/official_texts_19552.htm (accessed on 23.04.2019);

[97] Research Division - NATO Defense College, Rome - No. 36 – May 2008;

[98] Review of the implementation of OSCE Commitments in the field of Disaster Risk Reduction, http://www.osce.org/secretariat/123189, p.20;

[99] Riga Summit Declaration http://www.nato.int;

[100] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. p.p 11-17. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (accessed on 05.04.2019);

[101] Strategic Concept For the Defence and Security of The Members of the North Atlantic

[102] Swedish Civil Contingencies Agency (2011), *A functioning society in a changing world: The MSB's report on a unified national strategy for the protection of vital societal functions,* https://www.msb.se/RibData/Filer/pdf/26084.pdf;

[103] Swedish Civil Contingencies Agency (2014), *Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure,* https://www.msb.se/RibData/Filer/pdf/27412.pdf;

[104] Swedish Civil Contingencies Agency (2016), *Protection of vital societal functions & critical infrastructure,* https://www.msb.se/RibData/Filer/pdf/27956.pdf;

[105] Swedish Civil Contingencies Agency (2019), About MSB, https://www.msb.se/en/About-MSB/;

[106] The Alliance's New Strategic Concept https://www.nato.int/cps/en/natohq/official_texts_23847.htm (accessed on 02.04.2019);

[107] The Alliance's Strategic Concept https://www.nato.int/cps/en/natohq/official_texts_27433.htm?mode=pressrelease;

[108] The North Atlantic Treaty. https://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed on 10.06.2019);

[109] United Nations Development Programme (2014) *Review of the implementation of OSCE Commitments in the field of Disaster Risk Reduction*, http://www.osce.org/secretariat/123189, p.8;

[110] United Nations Development Programme (2014) Review of the implementation of OSCE;

[111] United Nations Security Council (2016) *Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat*, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/92;

[112] United Nations Security Council Counter-Terrorism Committee (2017) Physical Protection of Critical Infrastructure against Terrorist Attacks, https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf;

[113] United States Government Accountability Office (2009), *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts by Sectors' Characteristics*, GAO-07-39, Washington, D.C., https://www.hsdl.org/?view&did=469089;

[114] United States Government Accountability Office (2017), *Critical Infrastructure Protection: DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning, GAO-18-62,* Report to Congressional Requesters, October 2017, https://www.gao.gov/assets/690/688879.pdf;

[115] Wales Summit Declaration, 05 September 2014. www.nato.int;

[116] Warsaw Summit Communiqué. 09 July 2016. www.nato.int;

[117] White House (1996), *Executive Order 13010 Critical Infrastructure Protection,* Washington, D.C., https://fas.org/irp/offdocs/eo13010.htm;

[118] White House (1998), *Presidential Decision Directive/NSC-63, Critical Infrastructure Protection, May 22, 1998*. Washington, D.C., https://fas.org/irp/offdocs/pdd/pdd-63.pdf;

[119] White House (2013), *Presidential Policy Directive 21 / PPD-21 Critical Infrastructure Security and Resilience,* Washington, D.C., https://fas.org/irp/offdocs/ppd/ppd-21.pdf;

[120] White House (2017), *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Index

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

Professor Roberto Setola

Univertsita Capmus Bio-Medico di Roma, Italy

25 years later, the set-up of the US PCCIP on July 15, 1996 turning the attention on Critical Infrastructure Protection (CIP), this book provides an overview on the different initiatives promoted on a national and international level to improve the robustness, the resilience and the service continuity capability of such vital systems. The book allows the reader to capture the complexity of this particular problem, stressing from one site the need of stronger coordination and information sharing among the different stakeholders and authorities, and from the other the presence of an "innovative" dimension of security where natural events and manmade attacks have to be managed in an holistic framework . Such an all-hazard perspective is at the base for the modern concept of critical infrastructure protection.

Associate Professor Jonas Johansson

Director of Centre for Critical Infrastructure Protection Research, Lund University, Sweden

A book ripe with important insights and lessons learned when setting up and implementing national critical infrastructure protection systems, based on a comprehensive overview of the history of critical infrastructure protection and crucial pointers for the future from an EU, NATO, US, and, with special emphasis, Balkan countries perspective. It captures and reflects upon challenges from a multidisciplinary perspective, however staying grounded in its policy perspective. The importance of the safety, security and resilience of our dynamic and constantly evolving critical infrastructures, is and will become even more pronounced in the future, the interconnectedness of which calls for cross-sectoral policy and cooperation at the highest level.