MARINA MITREVSKA, ROBERT MIKAC

# HANDBOOK
# ON CRITICAL INFRASTRUCTURE PROTECTION

Prof. Dr. Marina Mitrevska,
Assoc. Dr. Robert Mikac

**HANDBOOK**
**ON CRITICAL INFRASTRUCTURE PROTECTION**

Reviewer:
Prof. d-r *Zoran* KEKOVIĆ

Publisher:
CHAMBER OF REPUBLIC OF MACEDONIA
FOR PRIVATE SECURITY
50-ta Divizija str., no.34
1000 Skopje, Republic of Macedonia
www.obezbeduvanje.org.mk
info@obezbeduvanje.org.mk

For the publisher:
**Verica MILESKA STEFANOVSKA, MA**
President
of Chamber of Republic Macedonia for Private Security

Cover:
*Aleksandar* ATANASOV

Printing:
Pope Kompani, DOO Skopje

Circulation: 300

**MARINA MITREVSKA**

**ROBERT MIKAC**

# HANDBOOK
## ON CRITICAL INFRASTRUCTURE PROTECTION

Skopje, 2017

**CHAMBER OF REPUBLIC OF MACEDONIA**
**FOR PRIVATE SECURITY**
**50-ta Divizija str., no.34**
**1000 Skopje, Republic of Macedonia**
**www.obezbeduvanje.org.mk**
**info@obezbeduvanje.org.mk**

CIP - Каталогизација во публикација
Национална и универзитетска библиотека «Св. Климент Охридски», Скопје
355.45(035)

МИТРЕВСКА, Марина
Прирачник за обезбедување на критичната инфраструктура / Марина Митревска, Роберт Микац. - Скопје : Комора на Република Македонија за приватно обезбедување, 2017. - 63, 55 стр. ; 25 см

Насловна страна на припечатениот текст: Handbook on critical infrastructure protection / Marina Mitrevska, Robert Mikac. - Обата текста меѓусебно печатени во спротивни насоки. - Текст на мак. и англ. јазик. - Фусноти кон текстот. - Библиографија: стр. 55-59 ; Bibliography: стр. 50-54

ISBN 978-608-65990-5-8
1. Микац, Роберт [автор]
а) Критична инфраструктура - Државна безбедност - Прирачници
COBISS.MK-ID 103781898

# CONTENTS

# PREFACE

Starting from the concept of critical infrastructure as a general set of values and goods that are essential for the economy, state and society and whose disruption in functioning or destruction could cause long-term harmful consequences for the basic values of the society, the necessity for building a coordinated approach in creating a modern concept for critical infrastructure protection is clearly recognizable. Moreover, it should represent an utmost priority for the institutions of the system, but also for all stakeholders in the society.

The Chamber of Republic of Macedonia for Private Security has recognized protection i.e. security of critical infrastructure as the key challenge in the tendency for continuous improvement of the private security sector and has consistently incorporated it in its vision for development of the field.

Through previously determined concrete measures and guidelines for future investments of capacities and resources, critical infrastructure protection represents precisely one of the identified strategic goals for development of private security field in the Republic of Macedonia. Our systematic approach involves primary provision of preconditions for upgrading the normative framework for critical infrastructure protection and the second stage which involves creating practical solutions as a direct response to the needs.

Namely, the Chamber of Republic of Macedonia for Private Security practices a consistent practice of continuous improvement through enhancing knowledge, skills and competences, so that the portfolio of vocational training and seminars includes multiple activities in the field of critical infrastructure protection. Publishing activity of the Chamber adds value to its determination that professional advancement requires specific literature, intended for the direct performers in the field.

In context of the above stated, this handbook illustrates the commitment of the Chamber of Republic of Macedonia for Private Security for further investment in critical infrastructure protection. At the same time, the handbook represents realization of the needs of the immediate performers in the field, whose developed consciousness openly requires practical mechanisms for improving work, aiming at greater professionalization and strong guarantee for common safety of the citizens.

We sincerely hope that the contents presented in this handbook will satisfy the appetites of the private security providers, but at the same time we sincerely expect that this publication will also be a provocation for animation of the interests of all participants in the process of critical infrastructure protection in the Republic of Macedonia and beyond, because only by recognizing and accepting common responsibility, direct involvement, cooperation and joint action one can guarantee common security at global level.

President
***Verica Mileska Stefanovska, MA***

# INTRODUCTION

Critical infrastructure represents a term and concept that is often used in the contemporary world, while the need to secure the vital functions of the state determines the significance of criticality of a particular infrastructure. In that context, it should be emphasized that "critical infrastructure" encompasses resources that are necessary for the functioning of societies, such as: energy capacities, information and communication technology, water, transport, as well as the role of the private sector.

The challenges for critical infrastructure protection are numerous. For those countries that are just beginning to form the concept of critical infrastructure protection, the challenges are manifested in understanding its importance, developing the normative framework, identification, determination of the sector and individual critical infrastructure, establishing appropriate and quality protection measures. In Southeast Europe, especially in the countries that have gone through the process of disintegration of Yugoslavia and are still not part of the EU and NATO, and are still struggling with other priorities, the conceptual and normative field of protecting critical infrastructure is still underdeveloped. In those circumstances, as a legitimate issue and a prerequisite for successful realization of security, critical infrastructure protection should become part of the agenda of the Republic of Macedonia. Therefore, within the framework of the Handbook, an analysis of key aspects of critical infrastructure is offered, which should serve the Republic of Macedonia in the process of establishing the concept for critical infrastructure protection.

The issues of critical infrastructure protection in the Handbook are systematized in seven parts.

Within the **First part** entitled ***"Notional Determination of the Critical Infrastructure Term"*** the emphasis is put on the conceptual definition of the infrastructure as critical. In this context, both threats towards critical infrastructure and the need for critical infrastructure protection have been addressed. Moreover, this section comprises the part referring to the analysis of the Indicative Critical Infrastructure List.

In the **Second part** entitled ***"Protection of Critical Infrastructure in the European Union"*** the focus of the research is dedicated to the development of the critical infrastructure protection from the aspect of the European Union, the work of the institutions of the Union and the orientation of this domain for cooperation with the private sector. This section also includes the part referring to the Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Within the **Third part** entitled ***"Critical Infrastructure Objects and Functions from Special Interest"*** the emphasis is put on analysis of different approaches to strengthening resistance and critical infrastructure protection. This part of the analytical probing of critical infrastructure objects and functions of special interest is dedicated to the analysis of the energy sector, transportation sector, information and communication technology, water and the place and role of the private sector.

Within the **Fourth part** entitled ***"Threats and Risks towards Critical Infrastructure"*** the emphasis is put on the analysis of natural threats and risks towards critical infrastructure. It also contains the analysis of technical and technological hazards and anthropogenic threats and risks towards critical infrastructure.

Within the **Fifth part** entitled ***"Critical Infrastructure Protection"*** four key issues have been elaborated. First, the organization of critical infrastructure protection is analyzed. The second issue involves an analysis of institutions that are competent for critical infrastructure protection. In the next issue the emphasis is put on the critical infrastructure protection, that is, public-private partnership. The last issue is an overview of several programs and work procedures.

The **Sixth part** entitled ***"Critical Infrastructure Protection in the Republic of Macedonia"*** is dedicated to the analysis of the critical infrastructure protection in the Republic of Macedonia.

In the **Seventh part** entitled ***"Examples of Past Terrorist Attacks on Critical Infrastructure"*** the attention has been paid to examples of past terrorist attacks on critical infrastructure. It contains an analysis of the terrorist attacks in the United States, Madrid and London.

# 1 CHAPTER NOTIONAL DETERMINATION OF THE CRITICAL INFRASTRUCTURE TERM

## 1. DETERMINATION OF THE INFRASTRUCTURE AS CRITICAL

The term "critical infrastructure" is not universally defined. The need to ensure vital functions of the state determines the significance of criticality of a certain infrastructure. It is thought that the term "critical infrastructure" dates back to the mid-1990s and is closely related to energy security, telecommunications, energy systems, gas and oil pipelines, the economy, transportation, water supply and so on.[1] In this context, it should be stressed that "critical infrastructure" encompasses resources that are necessary for the functioning of societies, such as: energy facilities and networks, communication and information technology, finances, health, food, water, transportation, production, storage and transportation of dangerous goods and government facilities.[2] Protection of critical infrastructure, such as water, energy and telecommunications is of utmost importance. 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, that is, society.[3] This can be seen in numerous definitions of "critical infrastructure" in literature. Different states define critical infrastructure differently. 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.[4] Let us take a look at some of them.

1. In the United States, 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."[5]
2. 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.[6]
3. 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."[7]
4. National critical infrastructure of Croatia encompasses "systems, networks and facilities of national importance, where their termination of work or services may have serious conse-

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

[2] Commission of the EU,( 2004), p.4

[3] Levis, G., (2006), Critical Infrastructure in Homeland Security-Defending a Net-worked National, John Wiley&Sons Inc.Hoboken, New Jersey (USA), p.1

[4] Keković, Z., (2013), National Critical Infrastructure protection regional perspective, Belgrade, p.203

[5] Patriot Act, 2001

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

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

quences for national security."[8]

5. 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. [9]
6. In NATO, on the other hand, critical are considered assets, services and information systems which are vital for a nation and their destruction may endanger the security, economy, health, that is security of the nation in general or impede effective functioning of the states.[10]
7. In the EU, critical infrastructure is defined as "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."[11]

Having in mind the foregoing, one can conclude that there is still no universally accepted definition of the critical infrastructure term. The analysis has shown that there are slight differences in the definition when it comes to NATO member states or EU Member States. Therefore, we will try to single out several common elements, namely:

*The first element* refers to the fact that critical infrastructure represents a system, asset, services, etc., which are crucial for the normal functioning of the state in terms of economic, health, social and security needs.

*The second element* refers to the fact that different national authorities have produced a list of economic branches encompassed in the abovementioned definitions. In particular, they include water, food, energy, transportation, and priority is given to airports and railways, financial institutions, health and so on.

*The third element* stems from the need for controlling and developing critical infrastructures. In doing so, the emphasis is put on the goal of promoting an institutional approach. Particularly, the approach should be aimed at creating a critical infrastructure strategy framework.

## 2. THREATS TOWARDS CRITICAL UNFRASTRUCTURE

Nowadays, unlike the past, threats towards critical infrastructure have expanded into many sectors, namely:

- economy (especially in banking and finance);
- transportation (airports and railways) and distribution;
- energy;
- health care;
- communications;
- utility services;
- food supply;
- Government services, etc.

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

[9] Ibid.

[10] Bognar, B., (2009), The process of critical infrastructure protection, AARMS, Budapest, p.552

[11] European Union Council Directive (2008), On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, 23/12/2008.

Hence, it is easy to conclude that some of the critical elements in the abovementioned sectors are not specifically "infrastructure", but rather a network or supply chains, related to essential products or services. This is supported by the fact that the number of factors threatening different elements of the infrastructure is increasing.

Threats towards critical infrastructure can be divided in several groups and subgroups, that is:

- artificial;
- natural; and
- threats of technological nature. [12]

Artificial or organized actions with harmful intentions include: terrorism, abuse for political gain, abuse for economic gain, instigation of armed conflicts, riots and protests.

While threats of natural forces include: floods, fires, earthquakes, landslides and so on.

Threats of technological nature can be caused by knowledge or ignorance, intentionally or unintentionally, or by a technological error. These include: car accidents, disasters, nuclear explosions, release of biological agents that can cause mass infections, pandemics, and diseases affecting a large number of critical personnel.[13]

In theory, there are a number of methodologies that assist directly in the identification of specific threats, namely:

- identification of basic infrastructure;
- evaluation of threats;
- evaluation of critical infrastructure endangerment;
- risk assessment.[14]

## 3. THE NEED FOR CRITICAL INFRASTRUCTURE PROTECTION

The need to protect critical infrastructure, basically, stems from the globalization process and the expansion of terrorism.

This condition and need indicate the following:

*First,* there is a direct link between the threat of terrorism and protection of critical infrastructure;
*Second,* there is a need for each country to have a systemic approach to the existing infrastructure;
*Third,* it is necessary for the infrastructure to be defined as critical, due to the possibility to be a potential target equally of the three types of threat.

In this respect, the need for an adequate analysis of the necessity of critical infrastructure protection is imposed. In fact, the choice does not aim for the individual analysis to be extensive, nor inevitably representative, but the choice is made from two aspects:

- from the aspect of international status, where the EU means the most attractive, relatively new, economic, political and security actor and international phenomenon;
- from the aspect of the international system, where NATO means a political framework for an international alliance modeled to prevent or deter aggression or provide assistance in

[12] Bognar, B., (2009), The process of critical infrastructure protection, AARMS, Budapest, p.500

[13] Bognar, B., (2009), The process of critical infrastructure protection, AARMS, Budapest, p.500

[14] Marjanović, M. and Nađ, I. (2013) National critical infrastructure protection –regional perspective: Assesment of threats to critical infrastructure facilities from serious and organized crime, Belgrade, p.78-79

case of disasters or a wider scale accidents.

Hence, the main task of this analysis is to present, through an example, how the EU and one NATO member state regulate the protection of critical infrastructure.

The EU directs its security to Member States, but also to the neighbors since negative consequences for destruction and incapacitation of critical infrastructure may be shared. Therefore it is necessary to achieve a standardized level of security of critical infrastructures that would minimize the risk of disrupting the normal functions of the Member States of the Union. Generally speaking, this is achieved through cooperation in different forms and concepts of foreign cooperation at a primary focused level, due to global interconnection of certain sectors, which require a different approach, dialogue and exchange of best practices.[15]

On the other hand, the United States, as a leading NATO member state, regulate the need for critical infrastructure protection through an integral approach:

- by identifying, preventing and preparing to deal with threats to critical security;
- by reducing the vulnerability of critical infrastructure;
- by mitigating the impact on critical infrastructure.[16]

In this regard, the US Directive on Critical Infrastructure Protection has a special place because it identifies energy and communications systems as significant critical infrastructures. First of all, this is about connection with the functions that are provided within all critical sectors.[17] Thus, the US approach is guided by three strategic imperatives, such as:

First, clear functional relationships in order to promote national unity and strengthen critical infrastructure security.

Second, creating conditions for efficient information exchange.

Third, implementation and integration of analyses from previous operations related to critical infrastructure protection, in the interest of quality decisions.[18]

Regardless the motives behind the different views regarding threats towards critical infrastructure, the EU and the United States have managed to form a joint determination at two levels that define:

- which resources represent critical infrastructure; and
- what measures are needed for their protection.[19]

This should be accompanied by the fact that critical infrastructure protection requires significant human potentials. That is why the need arises to overcome many challenges, of which we would single out the following:

- critical infrastructure complexity;
- jurisdiction regulations;
- lack of accountability in the sectors, where a number of state and private institutions are primarily engaged;

[15] Alchevski Gj., (2016) Implementacija na sovremenite bezbednosni sistemi i proceduri vo razvojot na obezbeduvanjeto na objektite od vitalen interes za Republika Makedonija (so osvrt na aerodromskata bezbednost), Skopje, pp.36-37

[16] National Infrastructure Protection Plan (NIPP), (2013) Partnering for Critical Infrastructure Security and Resilience, Homeland security, USA, p.7

[17] Presidential Policy Directive, (2013) Critical Infrastructure Security and Resilience the White House Office of the Press Secretary, USA.

[18] Presidential Policy Directive, (2013) Critical Infrastructure Security and Resilience the White House Office of the Press Secretary, USA.

[19] Škero, M., Zaštita kritične infrastructure i osnovni elementi uskladivanja sa direktivom Saveta Evrope 2008/114/ES

- insufficient information exchange, primarily among institutions, which, on the other hand, increases vulnerability and affects directly the efficient approach to critical infrastructure protection;
- the quantum of knowledge and skills regarding critical infrastructure protection;
- interdependence of critical infrastructure sectors and so on.[20]

Therefore, in parallel with determining strategic imperatives, it is also necessary to provide a good assessment of threats, vulnerability and consequences for critical infrastructure, and above all, improvement of critical infrastructure resistance, that is, safe critical infrastructure from possible human, physical and cyber threats.

## 4. INDICATIVE CRITICAL INFRASTRUCTURE LIST

A precise specification of critical infrastructures has been determined within the EU and most NATO member states.

For instance, the Indicative List of the European Commission includes: energy, information and communication technologies, water, food, finances, public administration, transportation, chemical industry, etc.[21]

While within NATO member states, the Indicative List includes the following:

- in Germany: energy, telecommunications, information infrastructure, public health, food and water supply, banking, finances, transportation, emergency and rescue services, government institutions, police, customs, armed forces, etc.;
- in the United Kingdom: energy, telecommunications, government institutions, health, finances, transportation, emergency services, water and drainage systems, etc.;
- in the United States: energy, information, telecommunications, public health, food, water, finances, emergency assistance, government institutions, basic defense industry, chemical industry and hazardous substances, etc.[22]

The analysis shows that all approaches are the same or similar, the difference being in complementing certain specific sectors.

[20] Prezelj., I., (2008) Konceptualna opredelite v kritične infrastructure, Fakultet društvene vede, Ljubljana, p.13

[21] Green Paper on a European Programme for Critical Infrastructure Protection, (2005), Brussels, Annex II

[22] See: Alchevski Gj., (2016), pp.40-41

# 2 CHAPTER PROTECTION OF CRITICAL INFRASTRUCTURE IN THE EUROPEAN UNION

The critical infrastructure protection domain in the European Union has developed in several different parallel processes. There are two key directions, first is marked by individual development of this domain individually by member states without contact and coordination with the European Union, and the other direction is based on the policies and processes that the Union has initiated and strive to coordinate. The first direction has longer time frame and countries such as Great Britain, Sweden, Switzerland, Nederland, Germany and France started to develop it predominantly in the last quarter of the 20th century, trying to strengthen their own infrastructure on which depends their own functioning. The European Union began dealing institutionally with critical infrastructure at the beginning of the 21st century under the influence of the United States and after the terrorist attack on September 11, 2001. After that, the development of this domain from the aspect of the European Union is characterized by three processes that take place in parallel and, they are networked. This is necessary to consider in understanding this domain. Firstly, the Union is primarily trying to set its own footprint in the field of critical infrastructure protection; secondly, it seeks to develop cooperation with those Member States that have the most developed national policies; thirdly, the Union is trying to standardize the area, to equalize the direction and speed of development, and to share the common approach of all Member States. A lot of effort has been invested in these processes, because it was necessary to reconcile the very different views and understandings about the critical infrastructure, especially among the developed and older Member States and the newer members which just started to meet with critical infrastructure protection only at the stage of achieving full membership of the European Union.

The focus of this part of research is devoted to the development of critical infrastructure protection from the aspect of the European Union, the work of the Union institutions and the orientation of this domain to cooperation with the private sector.

## 1. COMMON FRAME FOR CRITICAL INFRASTRUCTURE PROTECTION

The European Union has started this process under the strong influence of the 2001 terrorist attack on the United States, Global War on Terrorism that followed and major terrorist attacks in Europe in 2004 in Madrid and in 2005 in London, and it has its initial discourse of observation and protection of critical infrastructure, tied to the defense of terrorism. This discourse was dominant in the early years of development of this domain at the European Union level.

Critical infrastructure and terrorism represent two terms and concepts that are frequently used in the contemporary world. Their interaction is in the fact that many of those who deal in the area of critical infrastructure are trying to protect the said from terrorism. Many authors consider terrorism to be the leading threat to critical infrastructure while Elsa Lee goes even further and believes that terrorists' main targets in the United States of America (USA) and most of the western countries are critical infrastructure.[23] Official policies of many countries and organizations in the field of critical

[23] Lee, E. (2009) *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure*

infrastructure protection have been formed in the same way. Nevertheless, the said approach has certain cracks, starting with the inadequate terminological distinctness, conceptual underdevelopment of the critical infrastructure protection system, all the way to the inadequate national and international cooperation in critical infrastructure protection. The mentioned phenomena are especially visible within the countries that are deficit with the normative frame of the critical infrastructure protection, are lacking main strategic documents in the area of national security or they are not updated, or are in certain measure unstable, whether from internal or external reasons.[24]

Challenges in critical infrastructure protection are numerous. For the countries that are only beginning the formation of the critical infrastructure protection concept the challenges are manifested in understanding the importance of how the mentioned is important, developing the normative frame, identification, designation of the sector and individual critical infrastructure, establishing adequate quality/cost measures of protection. In the area of the Southeastern Europe, especially in the countries that have come to be through the process of the disintegration of Yugoslavia and are still not the part of the EU and NATO, still struggling with other set of priorities, conceptual and normative field of critical infrastructure protection is still undeveloped.

The Centre for European Policy Studies Task Force on Critical Infrastructure Protection from the organizational aspects of critical infrastructure protection, challenges sees in: relationship between the public and the private sector; unbounded, specifically in the case of critical information infrastructures there are no physical barriers or political boundaries; increasingly networked; complex; dependency on decisions brought by people and vulnerability.[25]

After the initial several years of consideration of this domain, the European Union has started with normative arrangement. Thus, in 2004, European Commission passed *Communication on Critical Infrastructure Protection in the Fight against Terrorism* in which the recommendation what Europe should do to prevent terrorist attacks on critical infrastructure, raise its resilience and develop the ability to answer the attack were laid out.[26] A year later the Commission passed *Green Paper on the European Program of Critical Infrastructure Protection* in which the solutions for establishing program for the critical infrastructure protection and creation of information alert network in case of threats to critical infrastructure have been proposed.[27] Then, in 2006, the Commission passed *European Program of Critical Infrastructure Protection* in which all the dangers to critical infrastructure were considered, but the terrorism has remained the primary focus and concern.[28] The Council of the European Union, in 2007, made a decision on establishing a special program, *The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risk*, as a part of the General program of security and protection for the period from 2007 to 2013. The Program recognizes numerous risks tied with security and in the middle, there is a part dedicated to support of members states' efforts to prevent terrorist attacks, prepare for protection and protect the people and critical infrastructure from

*Protection*, Boca Raton, Taylor & Francis Group: Auerbach Publication.

[24] Perinić, J. and Mikac, R. (2014) *Protection of the critical infrastructure from terrorism: Case study of the Republic of Croatia*, in: Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection, NATO Science for Peace and Security Series: Information and Communication Security.

[25] Heammerli, 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 (cited 5 May 2017).

[26] European Commission (2004) *Communication on Critical Infrastructure Protection in the fight against terrorism,* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702 (cited 6 May 2017).

[27] European Commission (2005) *Green Paper on the European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576 (cited 6 May 2017).

28 European Commission (2006) *European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786 (cited 6 May 2017).

risks related to terrorist attacks.[29]

As it can be seen the Union has focused its initial discourse primarily on the defense against terrorism. In time, the other risks were more and more acknowledged and considered, but terrorism has remained declared as the main threat.

## 2. DIRECTIVE 2008/114/EC ON THE IDENTIFICATION AND DESIGNATION OF EUROPEAN CRITICAL INFRASTRUCTURES AND THE ASSESSMENT OF THE NEED TO IMPROVE THEIR PROTECTION

The aforementioned discourse was dominant until 2008 when *Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* was enacted, which is now the key document for critical infrastructure domain in Europe, and it is no longer primarily focused on the threat of terrorism, but is endeavoring to completely set up the process of critical infrastructure protection on the level of the member states as well as the Union as a whole.[30]

According to the 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”. The 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”.[31]

The question is how to determine critical infrastructure from the aspect of criticality and respectively, national importance. There are two criteria that are more important than others. First, the attribute should be critically considered as something of special importance and without which it is not possible to function. Second, if we determine too many attributes which are critical, criticality is decreasing. On this behalf, it is worth pointing out the risk that the states which are inexperienced in these issues and those involved for the first time in the process of identifying and determining critical infrastructure, will overestimate the importance of some infrastructures and determine too much infrastructure in the critical category. An additional challenge arises because of the limited institutional capacities available for this activity, which greatly impedes a comprehensive approach to the protection of critical infrastructures. Defining national importance is variable and expansive concept and represents a framework for observing material, immaterial, virtual and intellectual objects, systems and values that, for certain criteria, can be assumed that their interruption of work, disruption of work or alienation would have significant consequences on national security, the health and lives of people, property and the environment, economic stability and the continuous functioning of the government. Such a widely-conceived concept brings us to the challenges of rational visualization because depending on the context of space and time, lot of this can be underlined as critical infrastructure.

[29] Council of the European Union (2007) *The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007D0124 (cited 6 May 2017).

[30] 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 (cited 1 May 2017).

[31] Ibid, p.174.

The Directive 2008/114/EC has been applied by the EU Member States since 12 January 2011 in the energy and transport sectors, with the perspective of expanding its application on other critical infrastructure sectors. All new members of the European Union are obliged to implement this Directive in national legislation before the accession to full membership of European Union.

The document is conceived as the first measure for identifying, determining and evaluating needed protection of critical infrastructure and this obligation and responsibility is assigned to the states and owners of critical infrastructure. The Directive seeks a unique approach to critical infrastructure protection with implementation in three phases: 1) Identification of potential critical infrastructure; 2) Determination of critical infrastructure; 3) Critical infrastructure protection. Thereby, the definition of critical infrastructure needs to be carried out through sectoral and inter-sectoral measures by analyzing business continuity risk where inter-sectoral measures include three criteria: human losses; economic losses; impact on the public. The Directive very clearly points out that it is necessary to make an analysis of business risk and safety plans in the protection of critical infrastructure and to identify security coordinators and national contact points for communication with the Commission and other countries. Although it is focused on the energy and transport sectors, Member States are given possibility to identify within the national framework additional sectors where it is possible to identify and determine critical infrastructure. Among other things, the Directive gives emphasis on the involvement of the private sector in the protection of critical infrastructures (supervision, risk management, business continuity planning, disaster recovery).[32]

## 3. THE ROLE OF THE PRIVATE SECTOR IN CRITICAL INFRASTRUCTURE PROTECTION

Public-private partnership is the key link in the implementation of critical infrastructure protection policies because most of such infrastructure is private property, all are dependent on it, and no company in the world is able to protect its own property by itself from all the possible risks that are potentially threatening without the cooperation of the public sector. Developed countries with developed policies of critical infrastructure protection view a public-private relationship as a necessary and extremely important element of the overall activities in the area of critical infrastructure protection. However, during the process the transition countries are– beside the lack of strategic frame for the public-private partnership in critical infrastructure protection – meeting with open questions of identifying, determining, ways and models of protection, but also the property of critical infrastructure.[33]

As it has already been said, in developed industrial countries of Western Hemisphere, the owner and manager of most critical national critical infrastructures is the private sector. Therefore, the challenge of critical infrastructure protection is additionally emphasized. The 2002 National Strategy for Homeland Security of the United States, highlights that the private sector is the major state supplier of goods and services and owns 85 percent of critical national infrastructure and by that, it is a key partner for achieving national security.[34] The British critical national infrastructure is predominantly privately owned. Realization of national goals depends on close co-operation between the public and private sectors, and the private sector is the crucial for protection of UK and British interests.35 In addition,

[32] Ibid.

[33] Perinić, J. and Mikac, R. (2014) *Protection of the critical infrastructure from terrorism: Case study of the Republic of Croatia*, in: Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection, NATO Science for Peace and Security Series: Information and Communication Security.

[34] Office of Homeland Security (2002), *National Strategy for Homeland Security*, https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf (cited 12 May 2017), page viii.

[35] Home Office (2009), *National Counterterrorism Strategy*, *Government of the United Kingdom,* http://tna.

the private sector with the function of managing critical infrastructure also has the responsibility to ensure its protection. Withal, the private sector is a major investor in critical infrastructure. Proportions of investment are visible on example of National Grid Company, which plans to invest [35] billion pounds in critical infrastructure on the United Kingdom and United States markets in period from 2013 to 2021. The critical infrastructure protection policies of the United Kingdom and the United States are quite similar because they follow the same logic originated from the strategic partnership, strong linkages between the British and American economies, common values and goals.

Transitional countries, with the lack of strategic documents in the area of national security, have difficulties because they did not notionally define what critical infrastructure represents and do not have clear public-private partnership concept on behalf of managing and protecting critical infrastructure. It is worth pointing out the opinion of the group of authors from Serbia who are observing the complexity of the problem through three prisms: cases of heavy economic crime within companies that represent potential critical infrastructure, lack of public-private partnerships in critical infrastructure protection, high levels of politicized management in such companies.[36]

Public-private partnership is a key link in the implementation of critical infrastructure protection policies, as the most of such infrastructure is private-owned, all stakeholders depend on it and there is no company which can without public sector co-operation independently protect its own assets from all possible risks which are potentially endangering it.

While all the consulted sources pointed out the importance of public-private partnerships in critical infrastructure protection, this relationship is laden by many challenges which Lee sets out on a general level as: mutual distrust; ignorance of procedures, powers and responsibilities; fear of exchange of information due the cases of "leaking" on both sides.[37]

For that reason, the Confederation of European Security Services (CoESS) has made White paper and guidelines named *The Public – Private Opportunity*. CoESS as the representative organization for European private security services, strongly believes there is a far greater role to be played by its members and their affiliated private security companies in securing and protecting critical infrastructure in a way which brings benefits to all – the responsible authorities, the infrastructure owners and operators, the end-users of critical infrastructure, the private security companies and the general public at large. In mention document CoESS highlights some examples of where public-private cooperation is functioning to the benefit of all stakeholders involved. It also contains suggestions on how these examples could be used as best practices and followed and implemented elsewhere. Finally, this document also provides guidelines for all parties involved on how to best secure and protect critical infrastructure.[38]

Cooperation between the public and private sectors is inevitable in the critical infrastructure protection domain. In the contemporary world which is burdened with increased number of asymmetric threats and risks, the co-operation of all elements of social power is simply a precondition that cannot be evaded. The states and societies which take that into account are more advanced and have more chances of success than those who do not use the public-private partnership model as a concept of implementation.

---

europarchive.org/20100419081706/http:/security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy-2009?view=Binary (cited 12 May 2017).

[36] Davidović, D., Kešetović, Ž. i Pavičević, O. (2012), *National Critical Infrastructure Protection in Serbia: The Role of Private Security,* Journal of Physical Security; 6(1), 59-72, Argonne National Laboratory, http://jps.anl.gov/Volume6_iss1/Davidovic.pdf (cited 14 May 2017).

[37] Lee, E. (2009) *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*, Boca Raton, Taylor & Francis Group: Auerbach Publication.

[38] The Confederation of European Security Services (CoESS), *The Public – Private Opportunity*, http://www.naftso.org/language/en/uploads/files/home__0/home__b12b429e50767e06715e1294ce238774.pdf (cited 16 May 2017).

# 4. THE REVISION OF DIRECTIVE 2008/114/EC ON THE IDENTIFICATION AND DESIGNATION OF EUROPEAN CRITICAL INFRASTRUCTURES AND THE ASSESSMENT OF THE NEED TO IMPROVE THEIR PROTECTION

Upon the adoption of the Directive, Member States have faced the challenge of adjusting national frameworks or for the first time establishing a whole set of programs related to the protection of critical infrastructures. Some consulted sources (Heammerli and Renda, Lazari and Simoncini) are considering that after the adoption of the Directive there was lack of further required steps from the Commission in the development of the area, and there was created a vacuum in which Member States were more or less left alone to act. More specifically, although the Directive makes clear provisions, monitoring of its implementation in national legislation is lacking. Alessandro Lazari and Marta Simoncini pointed out that the Directive is incorporated in each of the 28 national laws of the Union, namely through: 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); Declarations and executive orders (8 States), but not all countries have passed the norm of the Directive in the necessary manner.[39] Since the adoption of the Directive, the Commission did not have a clear objective how to guide and model the process.[40]

Although the Directive seeks to encourage Member States to closely cooperate, exchange information and good practice and to establish common European critical infrastructures (currently just over fifty critical European infrastructures are determined), the states are very difficult on deciding for such co-operation and they are retaining the policies of critical infrastructure protection predominantly within national borders. The Centre for European Policy Studies Task Force on Critical Infrastructure Protection deems that, even though the Commission has brought many political initiatives in this area, there still exist four major problems: ‘’First, member states are at varying degrees of maturity with respect to the development of a comprehensive and effective critical infrastructure protection 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.”[41]

The Commission has recognized the standstill in the process and revised the Directive in 2012, and in effort to make a breakthrough in the protection of critical infrastructure within the Union, in mid-2013 it presented a *Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure*, originally adopted in 2006. The Working document has a new perspective to more practical implementation of the *European Program for Critical Infrastructure*, provides an analysis of the elements of the current program and proposes a redefinition of the approach of critical infrastructure protection of the European Union, based on the practical implementation of activities within the area of

[39] 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 (cited 8 May 2017).

[40] Heammerli, 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 (cited 5 May 2017).

[41] Ibid, p.3.

prevention, preparedness and response. Part of the new approach is to perceive dependencies between critical infrastructure, industry and state entities, as it has been noted that the interdependence so far has not been sufficiently considered. For pilot-project of interdependence analysis, between various critical infrastructures important for the Europe, it was chosen: Eurocontrol, Galileo, electricity transmission network and gas distribution network. As many critical infrastructure is private-owned there is confirmed stance that better co-operation with the private sector is needed same as development of public-private structured dialogue. Additionally, four priority areas of the European critical infrastructure protection model are identified: 1) procedures for identifying and determination of critical European infrastructures and assessment of the need to improve their protection (detailed in Council Directive 2008/114/EC); 2) measures designed to assist the implementation of the *European Program for Critical Infrastructure*, including Action plan, Critical Infrastructure Warning Information Network (CIWIN), the use of expert groups for critical infrastructure protection at EU level, exchange of information, identification and analysis of interdependencies; 3) financing of measures related to the protection of critical infrastructures and projects associated with a special program for *Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*; 4) development of external dimension of *European Program for Critical Infrastructure* [42] With this new approach, the Commission seeks to improve the protection of critical infrastructure across the Union, raise up the entire process to a higher level and create a platform for sharing information and best practices by setting up expert groups for each sector.

[42] 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*, https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf (cited 21 May 2017).

# 3 CHAPTER

# CRITICAL INFRASTRUCTURE OBJECTS AND FUNCTIONS FROM SPECIAL INTERESTS

Each nation interprets and observes the objects of special interest for the functioning and defense of the country. There are various examples to consider and to take the best practice. In the Kingdom of Sweden, the term Critical Infrastructure refers to the activities, facilities, networks, infrastructure and services that maintain Vital Societal Functions. In that way, Vital Societal Functions is the term for the activities that maintain a given functionality. Each such function is included in one or more societal sectors. In Sweden, the primary focus is not on discussion on critical infrastructure objects but on functions that ensure their operationality. Sweden's national infrastructure is currently categorized by eleven critical sectors providing a set of critical societal functions.[43] In the Kingdom of Spain, the focus is set differently, from objectives to maintaining vital social functions. The CIP Law gives an official definition of what is to be considered as critical infrastructure: „The strategic infrastructures (that is, those that supply essential services) the functioning of which is necessary and does not allow alternative solutions, is the reason why their disruption or destruction would have serious impact on essential services". Spain's' national infrastructure is currently categorized by twelve critical sectors. Infrastructures have never been so important and influential for the normal functioning of services essential to the population and of main production systems as they are nowadays.[44] In the USA according to the *Patriot Act* 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 security, national economic security, national public health or safety, or any combination of those matters".[45] Where the focus of observation and protection is equally placed both on critical infrastructure objects and on their functions which are necessary for them to work effectively. The United States has sixteen sectors of critical infrastructure.

As shown in these three reference examples, there are different approaches to the strengthening of resistance and protecting critical infrastructure, depending on how each country decides what will be the focus. Some states are focused on the physical form, the other on the functions and the third on the observation of the overall situational image.

As practice has shown, not all sectors, objects and functions of critical infrastructure are equally important to the functioning of the state and society, and individual states like the US have decided to prioritize them in a way to distinguish certain lifeline functions that are essential to the operation of most critical infrastructure sectors. These lifeline functions include communications, energy, transportation, and water.[46] In the meantime, Spain identified 12 sectors in which critical infrastructure

[43] 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 (cited 15 May 2017).

[44] For more information see: Spanish Parliament (2011) *Law 8/2011 by which measures for the Protection of Critical Infrastructure Protection*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf (cited 16 May 2017), Ministry of Interior (2011) *Regulation for the Protection of Critical Infrastructure*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf (cited 16 May 2017).

[45] United States Congress (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA PATRIOT Act),* page 401, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (cited 15 May 2017).

[46] Department of the Homeland Security (2013) *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (cited 17 May 2017).

could be identified and in each of them determined at least one or more. The specificity is that the Spaniards make the difference between strategic infrastructures and critical infrastructures. They have around 4000 strategic infrastructures and around 400 critical infrastructures, where critical are more important than strategic.

In discussion regarding this topic, it is important to mention and process those sectors and examples that are more significant than others, whether by intermediation of *Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,* certain sector of energy and transport which are obligatory to perceive and analyze or as on the US example, to take into consideration lifeline functions (communications, energy, transportation, and water) which have an advantage over others. It is important to point out in the analysis of all approaches of different organizations and states, those key policies and processes that are essential for functioning whether the physical objects of critical infrastructure, or vital functions to which they contribute. Therefore, here will be elaborated examples for: energy, transportation, information and communication technology and water.

## 1. ENERGY SECTOR

Energy infrastructure is subject of European and national legislation and risk assessment to determine its criticality, reflecting its strategic importance. Basic philosophy on European critical energy protection comprises the following three points: A) Belief in a common and holistic approach to protecting infrastructure of strategic trans-boundary importance in Europe. B) All Member States have faced a constant increasing number of attacks on their critical energy infrastructure, mostly in the form of thefts, vandalism, and cyber-attacks. C) Owners and operators share the same goal (ensuring "efficient and secure operations at all times all around Europe") without exceptions. This requires openness and equal sharing of information between operators, owners, and state authorities.[47] The European Commission put its focus on linkage of Member State in this field, by financing certain projects as well as publishing studies and reports that can contribute to the improvement of the observed field.[48]

Just like the European Union, NATO also considers the significance and importance of the energy sector. The energy sector relies on a large number of diverse categories of infrastructure, which make up all the different components of the energy chain. These include infrastructures for the extraction, production or generation of energy, infrastructures for land and maritime transport, for processing and refining, for storage, distribution, etc. The energy sector also includes several sub-sectors – gas, oil, coal and electricity, each with its specific infrastructures. For instance, infrastructures for electricity production include facilities based on gas, oil, coal, hydropower, nuclear power, wind or other sources. In terms of protection needs, electricity is generally considered a more diversified, and, therefore, less attractive, sub-sector for terrorists, whereas the oil sector is more attractive, because of the high dependence of developed countries on foreign oil, mainly for transportation.[49]

The attractiveness of the energy infrastructure to terrorists is a result of the characteristics mentioned above – interdependence of energy infrastructures, dependence of other vital services and

[47] European Commission (2012) *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 (cited 17 May 2017).

[48] For more information see webpage of Directorate-General Migration and Home Affairs https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en, and webpage about Energy https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure (cited 16 May 2017).

[49] NATO Parliamentary Assembly (2008) *Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures,* http://www.nato-pa.int/Default.asp?SHORTCUT=1478 (cited 18 May 2017)

sectors on energy, dependence of Western economies on energy infrastructure located in unstable regions. Even though an attack on a major energy infrastructure might not necessarily cause many victims – though this obviously depends on the target, the economic cost and disruption are likely to be enormous. In fact, its impact can be amplified several times disrupting the targeted infrastructure; having a cascading effect on other energy infrastructures downstream as well as on other sectors of the economy; having a psychological impact upon and being amplified by the media; and potentially causing an overreaction of financial markets. Terrorists have also demonstrated their capability to attack energy infrastructures worldwide, although not all plots have been successful.[50]

As it is shown in introduction and now in this part of the chapter, states and multinational organizations are well aware of the importance of the energy sector for maintaining the existing level of development, the needs of public and national security and the prosperity of citizens. Nowadays, it is more impracticable to stop existing progress because as individuals, societies and states we are oriented towards new energy sources and maintenance of existing ones. In this activity, a significant partner is most certainly the private sector, to which the special attention will be paid in this chapter.

## 2. TRANSPORTATION SECTOR

Transportation systems is one sector, including: aviation, highway infrastructure and motor carrier, maritime transportation system, mass transit and passenger rail, pipeline system, freight rail, postal and shipping. Transportation is a key economic sector; it facilitates the movement of people, food, water, medicines, fuel, and other commodities. It faces multiple threats, ranging from accidents, failures or human errors to malevolent actions, namely sabotage, insider threats or terrorist attacks. Examples of the latter are the events in New York and Washington (2001), Madrid (2004), and London (2005). The common element of these incidents is the use of components of the transport infrastructure. In several cases, transportation components were used as the main means for the attack; in other cases, they were used as the target, which included cyber-attacks, too. Potential threats include the disruption of a mega node in the transportation network, the use of a transport component as an attack method and the release of a biological agent at a major passenger facility (rail station, ferry terminal, hub airport).[51]

We depend on transport on a daily basis but the transport should be considered as well as any other development platform (same as it was in previous section for the energy sector) in its interdependence with other sectors. The energy sector depends on transport in terms of securing traffic directions, technologies and techniques for the transport of energy sources from their source to the destination. On the other hand, the transport sector is largely dependent on energy sources in order to carry out its necessary activities. And they all depend on and are interlinked with IT and communication technologies without which today is not possible to have a viable high-efficiency business.

The significance of the transport sector excellently describes the American example that includes both actors and data that is needed to be taken into account in order to observe all the width of the subject field. The Transportation Systems Sector – a sector that comprises all modes of transportation – is a vast, open, interdependent networked system that moves millions of passengers and millions of tons of goods. The transportation network is critical to the USA way of life and economic vitality. Ensuring its security is the mission charged to all sector partners, including government (Federal, State, regional, local, and tribal) and private industry stakeholders. Every day, the transportation network connects cities, manufacturers, and retailers, moving large volumes of goods and individuals through a complex network of approximately 4 million miles of roads and highways, more than 100,000 miles

[50] Ibid.

[51] Theoharidou, Marianthi; Kandias, Miltiadis and Gritzalis, Dimitris (2012) *Securing Transportation-Critical Infrastructures: Trends and Perspectives*, https://pdfs.semanticscholar.org/5441/f94eb1dbb98f9fa4031c52ef3e476f71050b.pdf (cited 19 May 2017).

of rail, 600,000 bridges, more than 300 tunnels and numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports.[52]

In this example, it is necessary to draw attention to the specificity in deliberation and protection of critical infrastructures. When we see how large numbers in the US case are, although as a country they have large resources (but they are not unlimited), it is necessary to pay special attention to the values and sizes that will be determined as critical infrastructures. Because it is not possible that everything is protected as it cannot be protected by the same approach. Therefore, when critical infrastructures are defined, additional prioritization needs to be done to determine to what will be drawn more attention in relation to other infrastructures. And in this case, the role of the private sector is irreplaceable, concerning advanced nations.

## 3. INFORMATION AND COMMUNICATION TECHNOLOGY

Over the years, with technological development, information and communication technology has become an integral part of many critical infrastructure elements in all organizational sectors, from public to private. Today's world and its further development are unimaginable without information and communication technology. We are so attached and relying on this sector that it can be concluded that we are dependent on it in such scope and extent like no other sector. Here is also seen the interconnection, and we can even say – dependence on the private sector which mainly develops, produces, maintains, and upgrades contemporary systems that we take for granted and use on a daily basis. Another indicator is that public-private partnership is a platform for successful development at all levels of the society.

Although the use of ICT infrastructure has a positive effect on development of functional capabilities of systems, a large upgrowth of interconnected devices and information flows also increases the vulnerability of object and other critical infrastructures interconnected, primary by exposure to cyber threats and ICT infrastructure malfunctions. The systems and infrastructures are becoming very fragile and more risk prone which can cause dysfunctionality and furthermore can result with the large technological collapse.

The early Green Paper by the European Commission on critical infrastructures contains an example list of critical sectors, products and services. For the critical Information and Communication Technologies sector, seven products and services are listed: Information system and network protection, Instrumentation, automation and control systems (SCADA etc.), Internet, Provision of fixed telecommunications, Provision of mobile telecommunications, Radio communication and navigation, Satellite communication, and Broadcasting. Nations such as the Netherlands, who have detailed their critical telecommunications or information and communication technology sector in critical services and products, recognize fixed telecommunication services, mobile telecommunication services, internet access, satellite communication, and media/broadcasting as critical infrastructure services for their nations. Other nations only define their set of critical sectors or define the services and products at a high level. Switzerland, for instance, recognizes the following three ICT subsectors: information technologies (IT), media, and telecommunication. The US in its critical infrastructure sectors includes also the Communication sector and the IT sector. The critical Communication sector comprises wireline, wireless, satellite, cable and broadcasting infrastructures; the critical IT sector comprises the provision of IT products and services, incident management capabilities, domain name resolution services, identity management and associated trust support services, Internet-based content, information and communication services, and Internet routing, access and connection services.[53]

[52] Department of the Homeland Security (2007) *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, https://www.hsdl.org/?view&did=474328 (cited 17 May 2017).

53 Luiijf, Eric and Klaver, Marieke (2015) *Governing Critical ICT: Elements that Require Attention*,

## 4. WATER

Water is a key segment of life while water infrastructure is considered as one of the most important critical infrastructure on a global basis.[54] The public uses water for the most basic human needs. Vital networks and businesses, industries, hospitals, other utilities, agriculture, and manufacturing industries are dependent on water systems. Water systems are also essential to recovery efforts following any natural disaster and for maintaining the standard of living for our everyday lives.[55] As the world's total population grows, increasingly there will be more need and pressure on the water systems. Many people today do not have access to clean water and because of that people are suffering. Combined with global climate change, advance environmental pollution and decreasing cultivable land, large number of people are forced to permanent migration which increases demand for more robust water systems that will meet ever-growing needs. There are many conflicts over the water, for example in the Middle East, and more attention is devoted to protecting water systems from threats of terrorism.

Like every other sector of critical infrastructure, water sector also has some of the most important segments that need to be considered in order to get a clearer picture of the components we are discussing as a whole as well as the objects that need to be protected. Four components in the design of a public water supply system pertain to the safety and security of drinking water. They are: Raw water supply, including associated pipelines; Treatment systems; Distribution systems; Operation and control systems.[56]

Water critical infrastructure is strongly connected and dependent on some other previously discussed sectors, such as information and communication technology, same as on electrical energy. Equal as other critical infrastructure sectors, water critical infrastructure is vulnerable to a variety of natural and human-caused threats. People may question the need to secure pump stations, water storage facilities, treatment plants, or pipelines. The simple response to this reflection is that the negative consequences of an intentional attack are too great to ignore. A significant attack on a water system could result in widespread illness or casualties. A denial of service scenario could affect critical services such as firefighting and health care and could disrupt other dependent sectors such as energy, transportation, and food and agriculture.[57]

## 5. THE PLACE AND ROLE OF THE PRIVATE SECTOR

Over the time, there is growing awareness of the need for synergy between the public and private sector in the construction, maintenance and protection of critical infrastructures. Since the beginning of the development of this field, the European Commission has been very clear about the

http://societalsecurity.net/sites/default/files/document-database/files/2016-03/pdf/3018787-governing-critical-ict-elements-require-attention.pdf (cited 21 May 2017).

[54] Birkett, D.M. (2017) *Water Critical Infrastructure Security and Its Dependencies*. Journal of Terrorism Research. 8(2), pp.1–21. DOI: http://doi.org/10.15664/jtr.1289 (cited 24 May 2017).

[55] Van Leuven, Laurie (2011) *Water/Wastewater Infrastructure Security: Threats and Vulnerabilities*, https://www.researchgate.net/publication/226050430_WaterWastewater_Infrastructure_Security_Threats_and_Vulnerabilities (cited 24 May 2017).

[56] Public Safety and Emergency Preparedness Canada (2003) *Water, Critical Infrastructure Protection and Emergency Management*, http://publications.gc.ca/collections/collection_2008/ps-sp/PS4-7-2004E.pdf (cited 19 May 2017).

[57] Van Leuven, Laurie (2011) *Water/Wastewater Infrastructure Security: Threats and Vulnerabilities*, https://www.researchgate.net/publication/226050430_WaterWastewater_Infrastructure_Security_Threats_and_Vulnerabilities (cited 24 May 2017).

need for joint work of the public and private sector. Thus, in 2004 European Commission pointed out how Europeans expect critical infrastructures to continue to function, regardless of which organizations own or operate the component parts. They expect the Member State governments and the EU to play a leadership role in ensuring that this happens. They expect all levels of government and private sector owners and operators to cooperate to assure the continuity of the services on which Europeans depend. Where success, among other indicators, also shall be measured by: The European Community resolves to establish a common approach to tackling the security of critical infrastructures through cooperation of all public and private actors.[58]

In the next significant document *European Program of Critical Infrastructure Protection,* the European Commission was not so explicit regarding cooperation of the public and private sector which is mentioned in the of public-private dialogue concerning critical infrastructure protection as well as participation in Expert groups that would advise the Commission on essential matters.[59] However, in the most important document in this field, *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (Directive 2008/114/EC) the Commission has briefly but very strongly emphasized the importance and role of the private sector. Given the very significant private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery, a Community approach needs to encourage full private sector involvement.[60]

Individual consulted institutions and authors strongly believe in the need of this partnership. For example, some authors believe that inclusion of the private sector is imperative. They emphasize that approx. 90% of national critical infrastructures are actually in the hands of the private sector. Moreover, they believe that the companies in the private sector are best placed to assess what systems and subsystems within their own business or sector require special protection.[61] Centre for European Policy Studies emphasizes how there is no way to organize a meaningful critical infrastructure protection policy without involving the private sector, as critical infrastructures in Europe are mostly owned by private players, many of which are worldwide operating companies.[62] While on the implementation side of critical infrastructure protection CoESS highlights how securing and protecting critical infrastructure is one of the most suited areas for public-private partnerships, given their often public (national or local) character, which is translated in public ownership or public management or public objective. As an increasing number of security functions, which were previously carried out directly by public authorities, are contracted out, private security companies are becoming increasingly involved in ensuring public security, including in critical infrastructure.[63]

[58] European Commission (2004) *Communication on Critical Infrastructure Protection in the fight against terrorism,* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702 (cited 6 May 2017).

[59] European Commission (2006) *European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786 (cited 6 May 2017).

[60] 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 (cited 1 May 2017).

[61] Brömmelhörster, Jörn; Fabry, Sandra and Wirtz, Nico (2004) *Critical Infrastructure Protection: Survey of World-Wide Activities*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.html (cited 17 May 2017).

[62] Heammerli, 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 (cited 5 May 2017).

[63] The Confederation of European Security Services (CoESS), *The Public – Private Opportunity*, http://www.naftso.org/language/en/uploads/files/home__0/home__b12b429e50767e06715e1294ce238774.pdf (cited 16 May 2017).

# CHAPTER 4

# THREATS AND RISKS TOWARD CRITICAL INFRASTRUCTURE

Critical infrastructure represents networks, objects and systems distributed in expanse, whose business continuity is influenced by numerous natural, techno-technological and anthropogenic factors. In order to protect them in best way, it is necessary to consider the most significant threats and risks categorized in the above listed groups. In addition, special attention needs to be devoted to the dependence and interdependence of critical infrastructure operability arising from the effects of the very nature, structure and business processes that affect critical infrastructure. Different areas in the world have their own specific natural threats and the risks that recur, interact with others, and pose a potential and/or direct threat to critical infrastructures. It is needed to observe individual analyzes and cost calculations to obtain a situational picture of threats and risks that, in addition to other values, threaten critical infrastructures. The area of Southeast Europe because of its natural position is a zone that is extremely vulnerable to natural threats such as flood, earthquake and fire. In the last ten years, floods are the biggest threat. Of technical-technological hazards, it is necessary to distinguish: disasters and major accidents in economic facilities; technical-technological disasters and major traffic accidents; nuclear hazards. And anthropogenic factors are distinguished as follows: acts related to terrorism, sabotage and crime. Where there are empirical evidence, examples from the Southeast Europe region and occasionally the wider context will be used.

## 1. NATURAL THREATS AND RISKS TOWARDS CRITICAL INFRASTRUCTURE

United Nations Development Programme in its research, states how the area of the member states Organization for Security and Cooperation in Europe, is very susceptible to natural disasters – such as earthquakes, floods, droughts, storms, thermal waves, forest fires – which have been affecting more than 76 million people over the last 25 years. According to analyzes from 1990 to 2014, storms (34 percent) and floods (31 percent) are most common natural disasters. Floods (35 percent), storms (29 percent) and droughts (19 percent) affect most people in the named area. Due to the earthquakes (54 percent), the floods (26 percent) and the storms (16 percent), the largest number of people remained without their own homes. 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.[64] Margareta Wahlström, Special Representative of the Secretary-General of the UN for Disaster Risk Reduction said, estimation is that global annual economic losses caused by natural disasters are greater than $ 100 billion USD and trends shows that it will continue to grow. Christian Friis Bach, UN Secretary-General of Economic Commission for Europe, has given the data on 100 billion Euro losses in the EU for the last ten years that have been caused by natural disasters. For the same period, the European Commission estimates that natural disasters in the European Union between 2002 and 2014 have caused more than 80,000

[64] 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, page 8 (cited 21 May 2017).

deaths and more than 100 billion Euros in economic damage.[65]

Between numerous major natural disasters, statistically, floods represents the phenomena which very frequently and cumulatively cause great damage, economic and human losses, significant security and health challenges, numerous consequences for people, economics, critical infrastructure, the service sector, the environment and the historical heritage. According to the European Environment Agency report, from 1998 to 2009, 213 floods in Europe were reported, causing 1,126 deaths and economic losses of more than 52 billion Euros.[66] Some areas in Europe are more flood prone than others which can be seen in historical records, but also in the recent events. Over the past few years, floods have marked the area of Central and South-Eastern Europe. We are noting the historical water maxima on large European rivers such as the Danube, Tisza, Drava, Mura, Sava, and other rivers and their tributaries. The floods have caused multiple embankments breach, flooding of large defended area, human casualties and massive damage to property in dozens of states. According to the European Commission, Central Europe in 2013 experienced the hundred-year flood, i.e. the flood with the probability to occur once in a hundred years, and it is for the second time in only 13 years.[67] Equally, it is no longer rare that water meters in many watercourses in the European area are recording water levels which correspond to the likelihood of 200 and 500 year large waters. Due to the effects of climate change and persistent environmental degradation, it can be expected that more intensive and more frequent floods will occur.[68]

Similar situation happened in Southeast Europe where the most significant consequences manifested in 2014. In May's floods, which was that kind of flood which occurs once in every 1000 years, numerous areas in Bosnia and Herzegovina, Serbia and Croatia have been affected the hardest. 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, more than 1.6 million people were affected by floods, and 31 thousand were evacuated. In Croatia floods have endangered 38,000 people.[69] From the aspect of critical infrastructure, the mentioned flooding has caused many problems in the functioning of the water supply system, transport and processing sector, agriculture, education and health system. Some flooded areas have exhausted the local, regional, and even individual state capabilities and resources and states have received international assistance.

The area of Southeast Europe as a part of the Mediterranean-transitional belt excels by its expressed seismic activity. The feature of spatial distribution of seismic activity is the concentration of earthquakes in certain narrower areas or zones. This is especially valid for coastal areas and parts of the interior that have been affected by devastating earthquakes. We highlight several very powerful earthquakes marking this area. The earthquake that occurred in 1667, the intensity of the 10-degree Mercalli-Cancani-Sieberg (MCS) scale, when Dubrovnik was almost completely destroyed. More than 3,000 people were killed.[70] The earthquake in Skopje in 1963 caused more than 1,000 mortali-

[65] European Commission (2014) *ECHO Factsheet – Disaster Risk Management – 2014,* http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/disaster_risk_management_en.pdf, pages 1 (cited 21 May 2017).

[66] 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, (cited 22 May 2017).

[67] European Commission (2014) *ECHO Factsheet – Disaster Risk Management – 2014,* http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/disaster_risk_management_en.pdf, pages 1 (cited 21 May 2017).

[68] 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, (cited 22 May 2017).

[69] 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, page 20 (cited 21 May 2017).

[70] Government of the Republic of Croatia (2009) *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća*, http://www.duzs.hr/download.aspx?f=dokumenti/Stranice/PROCJENAUGROZENOSTIREPUBLIKEHRVATSKE.pdf, page 11 (cited 23 May 2017).

ties, more than 3,000 injured and between 120,000 and 200,000 people left without their own homes. The earthquake has destroyed between 75 and 80 percent of the city. The 1969 earthquake almost completely destroyed Banja Luka. Fifteen people were dead, more than 1,000 were strongly and easily injured. The earthquake in Montenegro in 1979, in addition to Montenegro area, caused casualties and material damage in Croatia and Albania. In the earthquake, 101 people died in Montenegro, 35 in Albania, and more than 100,000 people were left homeless. In all the above mentioned earthquakes, there were great material damage. From critical infrastructure aspect, significant damage has been recorded on numerous facilities, networks and systems from local to state infrastructure. Major damages have been caused to educational, cultural, health, social and public administration and administration facilities. Significant damages also occurred in the economy, even to the extent that certain businesses ceased fully with their activities.

The cause of the earthquake in the coastal part is the underlining of the Adriatic plate under the Dinarides as a result of the movement of the African plate towards the Euro-Asian plate. In the northwestern continental part, the causes of the earthquakes are compression processes due to the shift of the Dinarides and the Alps, while in other areas are caused by different movement of the masses of certain mountains. Although the area of Southeast Europe is exposed to the real risks of earthquakes, it is not the most active seismic area in the world. The Apennine Peninsula is experiencing constant earthquakes, resulting in human losses, material damage and discontinuation of work and damage to critical infrastructure. Seismically the most active zone is the area of the Pacific Ocean. In the earthquake that occurred in 2004 in the Pacific Ocean, and consequently caused tsunami in the area of Indonesia and neighboring islands, more than 227,000 people were killed. The earthquake with the same scenario occurred in 2011, after which Japan was stricken. The Nuclear power plant in Fukushima was also affected by domino effect, and more than 16,000 people died.

From the aspect of discussion about the taking certain measures and activities identified from these earthquakes, stands out the need for more resistant construction in order to minimize and avoid as much as possible, damage to housing, roads, local as well as critical infrastructures. Thus, the buildings masoned until 1920 had ceilings constructed exclusively of wood. The reinforced concrete ceilings were gradually made in the period from 1920 to 1940. From 1945 to 1964 prevailed reinforced concrete monolithic ceilings of semi-mounting types or made on-site. After 1964, the built-up buildings were systematically constructed with horizontal and vertical culverts, and the buildings of collective housing with reinforced concrete support system constructed in accordance with the provisions of the Seismic Regulations of 1964 (after the earthquake in Skopje), which can be considered as a modern way of construction in terms of the scientific knowledge at that time.[71] Special attention is devoted to building critical infrastructure from local to state level.

Fires of various feature pose a potential danger to all levels and forms of society and the economy. They potentially endanger a greater number of people and assets in all types of facilities where a large number of people gathers, in various modes of transport, in tunnels, in technology facilities and the infrastructures which stocks hazardous goods, same as in large open space fires. In the last ten years a particular danger in the area of Southeast Europe is open space fires. This danger is emphasized in drought periods, especially in the coastal part in the summertime. Due to climate change and their impact, we are increasingly witnessing major fires affecting Bosnia and Herzegovina, Serbia, Macedonia, and the interior of Greece.

Fires cause significant direct and indirect damage and their extinction sometimes requires the engagement of large material, technical and human resources of 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 capacity to extinguish them. They have direct consequences for certain critical infrastructure sectors such as: energy (production, including accumulation and

[71] Ibid, p.16.

dams, transmission, storage, energy and energy transport, distribution systems), traffic (road, rail, air, maritime and river) and public services (public order and peace insurance, civil protection system, emergency medical aid). While there are indirect consequences for other critical infrastructure sectors.

## 2. TECHNICAL-TECHNOLOGICAL HAZARDS TOWARDS CRITICAL INFRASTRUCTURE

Technical-technological major disasters and catastrophes with serious consequences to people, material and cultural goods as well as critical infrastructure can arise due to numerous causes as well as domino effects after the initial accidents. The most general classification of technical-technological major accidents and catastrophes shows all the width of the potential scenarios of endangering the values that we strive to protect. The above mentioned are divided into: technical-technological disasters and major accidents in economic facilities; technical-technological disasters and major traffic accidents; nuclear risk. Discussing this, it is needed to emphasize how in this case observed are disasters and major accidents which occur due to the negative factors of the technological process as well as unintended human fault.

In all countries, 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 known two examples which has marked this domain: a big Seveso disaster in 1976 and the disaster in Bhopal in 1984. The city of Seveso, in the north of Italy, was the site of one of the greatest chemical accidents in the history of mankind. A large amount of dioxin has been 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 the people about 1,800 hectares of soil contaminated, and an increased number of spontaneous abortions in the region have been reported in months of accident. Far the biggest chemical disaster occurred in the Indian city of Bhopal when a large amount of chemicals leaked from the pesticide factory due to a technological failure. The consequences were horrifying. More than 25,000 people died and more than 150,000 people have had serious illnesses, while to this day in that area, children of severe physical and mental disabilities are born more often than elsewhere.

The Seveso accident induced the European Union to stronger business regulation and control of chemical plants. This was done through Seveso Directive[72] which ensure 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.[73] The specificity of this approach in relation with consideration of the critical infrastructure protection aspect is that we have a demand for as much transparency as possible and publicly available indicators of all processes in chemical

[72] The first directive called Seveso I was adopted in 1982. Seveso II was adopted in 1996 and took into account the disaster in Bhopal. While Seveso III was adopted in 2012. Each new Directive has replaced the previous one and additionally stricter the regulation of the operation of chemical plants, which are currently more than 10,000 in the European Union.

[73] 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 May 2017).

plants while on the other hand the concept of critical infrastructure protection requires a certain level of confidentiality of structure and process data. When the same plant is appointed by the legislator as obligatory to apply Seveso Directive and as the object of national critical infrastructure, the plant meet the challenges in the process of fulfillment of both obligations none of which is simple and application is a partial collision in the principles of action.

Technical-technological disasters and major traffic accidents (road, rail, airborne, maritime and river) may arise due to the numerous processes taking place during the transport of dangerous substances as well as during their manipulation at the stands. Possible causes of danger from unexpected events can be estimated from the experience on accidents which has already occurred, namely: improper handling of vehicles in transport; incorrect load; defective transportations parts; inattention, neglect or negligence at work or improper handling; lack of process control; damage caused by mechanical shocks; failures on devices or errors when pulling and filling the container; fires on the objects, human intentional activities on the producing of the accidents. As an example of a technical-technological accident in traffic, we can mention an example of a Turkish cargo ship UND Adriyatik in 2008 near the western coast of Istria, Republic of Croatia. The ship carried a larger number of trucks to Trieste port and due to unidentified causes fire occurred. The crew could not stop the fire that spread and affected most of the cargo. They evacuated from the ship and UND Adriyatik floated for days carried with sea currents in the very narrow northern Adriatic Sea. After a few days, it was extinguished and the ship was towed to Italy. There was a real danger that the fire would result in the dissolution of the hull and the leakage of large quantities of chemicals into the sea. This would cause an ecological catastrophe and cause major direct damage to the tourism sector as one of the critical sectors of critical infrastructure when we consider Croatia's dependence on filling the state budget through this sector.

Nuclear accidents are a risk which needs to be considered with the utmost attention. Nuclear power plants, regardless of the type of plant contain large amounts of radioactive substances, thus posing a potential danger to humans, animals, the environment and the normal life cycle. Most of the radioactivity is related to the fission products found in the reactor core. Any uncontrolled release of radioactive substances from a nuclear power plant into the environment threatens the health and lives of the population and pollutes the environment. To the safety of nuclear power plants is paid a great attention, and risks are trying to be reduced to the smallest possible extent. However, experience so far has shown that irregularities, incidents, accidents and even disasters in nuclear power plants are still occurring.[74] Serious nuclear power plant accidents include the Fukushima Daiichi nuclear disaster (2011), Chernobyl disaster (1986), Three Mile Island accident (1979), and the SL-1 accident (1961).[75] As of 2014, there have been more than 100 serious nuclear accidents and incidents from the use of nuclear power. Fifty-seven accidents have occurred since the Chernobyl disaster, and about 60% of all nuclear-related accidents have occurred in the US.[76] In addition to this, numerous accidents occurred on Soviet nuclear submarines as well as radiological accidents around the world.[77]

[74] Government of the Republic of Croatia (2009) *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća*, http://www.duzs.hr/download.aspx?f=dokumenti/Stranice/PROCJENAUGROZENOSTIREPUBLIKEHRVATSKE.pdf, page 45 (cited 23 May 2017).

[75] TIME (2009) *The Worst Nuclear Disaster*, http://content.time.com/time/photogallery/0,29307,1887705,00.html, (cited 22 May 2017).

[76] Benjamin K. Sovacool (2010) *A Critical Evaluation of Nuclear Power and Renewable Electricity in Asia,* http://dx.doi.org/10.1080/00472331003798350, page 369-400 (cited 24 May 2017).

[77] For more infromation please see the International Atomic Energy Agency web page, http://www-pub.iaea.org/books/IAEABooks/Publications_on_Accident_Response, (cited 23 May 2017).

# 3. ANTHROPOGENIC THREATS AND RISKS TOWARD CRITICAL INFRASTRUCTURE

Anthropogenic threats and risks toward critical infrastructure are generally considered as acts related to terrorism, sabotage and crime directed at the functioning of whole or some parts of critical infrastructures.

Critical infrastructure represents a vast, global sector. It is therefore not possible to ensure its full protection at all times and in all places. Unfortunately, it is likely that some terrorist attacks against critical infrastructure will succeed. Terrorists aim to spread fear, anxiety and panic, creating the perception that every citizen and critical node in a country's infrastructure is vulnerable to attack. This was the case on 22 March 2016, when two teams of ISIL operatives conducted simultaneous attacks in Brussels, at Zaventem airport (killing 11 people) and at Maelbeek metro (killing 20 people), respectively. Around 300 people were injured.[78] Al-Qaida and its affiliates have attacked facilities and personnel of oil companies in Algeria, Iraq, Kuwait, Pakistan, Saudi Arabia and Yemen, and have also captured numerous oil fields. The UN estimates that the income generated by ISIL from oil and oil products in 2015 was between $400 million and $500 million.[79] Even though some authors note that energy attracts only a small share of terrorist attacks, trends suggest a sharp rise terrorists' interest in oil and gas.[80] According to numerous studies, more attacks in the world are directed toward critical infrastructures.

The next important anthropological threat is the act of sabotage which is the border occurrence between the terrorist act and the criminal act, and every case needs to be considered separately. Sabotages and terrorist attacks are major threats to critical infrastructures. These attacks usually target infrastructures such as energy production and transmission systems, food and water supply networks, telecommunications networks, transportation networks, etc. Methods of committing such acts can be arson, causing explosions, the use of weapons of mass destruction to even the most common forms of attack, various cyber-attacks. Hostile cyber-actors come in both state and non-state varieties: foreign intelligence agencies, terrorists, misguided hacktivists, or simply individuals acting alone. These hostile actors have access to a growing range of cyber-attack tools and techniques. As technologies evolve and become more complex, so too do the challenges of detecting and protecting against cyber-attacks. Although it is commonly considered that the main attackers via internet are hackers and/or terrorists, it is necessary to draw attention to state actors in this activity as well. Foreign intelligence agencies are making increasing use of the Internet to conduct their espionage operations: it is a relatively low-cost and low-risk way to obtain classified, proprietary or other sensitive information. The main targets are high-technology industries, including the telecommunications sector, the oil and gas industry and other elements of the natural resource sector, private sector, as well as universities involved in research and development have also occurred. State-sponsored attackers seek information which will give their domestic companies a competitive edge. State-actors have also been known to use cyber-attacks to disrupt political and economic activity as a means of influencing government decision-makers. Threats

[78] 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, page 3-4 (cited 2 June 2017).

[79] 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, (cited 2 June 2017).

[80] 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, (cited 2 June 2017).

from cyber-espionage, cyber-sabotage and other cyber-operations are part of a broader economic threat to key critical infrastructure sectors.[81]

Criminal activities toward the critical infrastructure can be divided into insider and outsider. Insider threats are part of each organization. Basically, this occurs when theretofore trusted employee betrays his obligations and loyalty to employer, conducting sabotage or espionage against them. This "insider betrayals" can be acts of theft as subtle forms of sabotage or more aggressive acts like work-place violence. The threat posed by insiders is a term that is commonly used in case of IT network use violations. This often leads to further confusion about the nature and seriousness of the threat.[82] External threats have already been partially described and they represent variety of attempts to infiltrate the system either physically or through the internet and the motive may be different depending on the motivation of the attacker. Physical intrusions matter the attempts of alienation of a piece of equipment or obtaining important information directly, by collaborating with company employees or by a certain type of fraud or extortion. But much bigger and more serious invasions are attempts to invade cyber space. Such attacks on critical infrastructure occur every day on a global scale and the trend is increas-ing. As the cyber space and critical infrastructure have become inseparable, security challenges are emerging same as consideration in which way is the best to protect vital parts of critical infrastructure from external intrusion. This strong correlation between internet and critical infrastructures comes at the cost of increased complexity and, as a consequence, increased risks of accidental faults.

[81] Canadian Security Intelligence Service (2017) *Cybersecurity and Critical Infrastructure Protection*, https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php, (cited 12 June 2017).

[82] 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, (cited 6 June 2017).

# 5 CHAPTER CRITICAL INFRASTRUCTURE PROTECTION

The protection of critical infrastructure is a very broad and dynamic activity carried out by public bodies, such as various legislative institutions, law enforcement agencies, inspection and judicial bodies, private security organizations, up to international bodies as the European Union and NATO. Every case is unique, so it is necessary to pay special attention to it and to perceive that many actors, at various stages and processes participate in its protection.

To illustrate the extent of discussion here concerned, it is needed to list the examples of critical infrastructure: 1.) Energy sector - nationally important oil and gas refineries; 2.) Transport sector - the largest airports; 3.) Information 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.) Sector of Water Management – Wellfields; 8.) Sector of production, storage and transport of hazardous substances – integrated monitoring and control system for the transport of hazardous substances; 9.) Public Services - Emergency Medical Assistance; 10.) Sector of Tourism – National Monuments that are the reason for the arrival of a large number of tourists.

As it is apparent, the critical infrastructure is very diverse and it is represented in networks, facilities and systems that are not always physically visible, but consist of many components and interdependencies, most commonly in the Web world. We can state an example of 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 doing an additional breakdown and we have to specify which processes are irreplaceable, whether there is an alternative to their action and what will happen if they stop or temporarily cease to operate. Thus, when we are talking about the protection of critical infrastructures, it is important to keep in mind that they are complex systems which require a holistic approach in considering their functioning, sources of their internal and external threats, importance for the sector itself, and dependence and interdependence with other sectors and critical infrastructures, strengthening their resistance as well as protecting them.

A key understanding of the overall protection of the state and society from the aspect of preserving the functioning of critical infrastructure is based on the „package of protection" of all infrastructures as well as each individual. Every infrastructure and entire country will be best protected if we diversify the supply and delivery routes as much as possible, create and strengthen alternatives to critical infrastructure and strengthen their resilience. Then we will protect such objects to build them in areas which are as less as possible risk prone to flood, fire and earthquakes. Also, to build them according to the rules of the profession and with the use of quality materials, respecting all construction and maintenance standards. The next step is to produce the complete supporting documentation and the knowledge of the processes in order to avoid standstills and domino effects. There is also the resistance of the system itself, its robustness and high functionality which are needed to be taken into account. Thereafter, the question arises of whether critical infrastructure has made all the necessary assessments, analyzes and plans required by other laws because national laws directly related to the issue of critical infrastructure are just an upgrade to everything which is previously done. It would certainly be good if the owner or manager of critical infrastructures has harmonized and/or improved their business to one of the international standards for business, quality management, crisis management and/or emergency management. Important question is also whether they have a crisis plan, a crisis communication plan, are they conducting internal exercises, are they linked up with urgent services,

and similar. Means, there is a whole range of required and previous undertaken activities with which by structural measures we are avoiding and reducing the vulnerability of critical infrastructures. As it is a very wide range of jobs and areas of responsibility, the private sector has a significant place in this scope.

## 1. ORGANIZATION OF CRITICAL INFRASTRUCTURE PROTECTION

The approach to critical infrastructure protection should be primarily based on risk analysis that needs to determine which risks jeopardize critical infrastructure operations and how to respond to these. Risk is a function of the likelihood of a given threat source displaying a particular potential vulnerability, and the resulting impact of that adverse event. Risk analysis refers to the processes used to evaluate those probabilities and consequences, and also to the study of how to incorporate the resulting estimates into the decision-making process. The risk assessment process also serves as a decision-making tool, in that its outcomes are used to provide guidance on the areas of highest risk, and to devise policies and plans to ensure that systems are appropriately protected.[83] Within the private sector, there are specialized companies working successfully in this field, so the existing collaboration between the public and private sector needs to be additionally developed to enable the private sector's knowledge and skills to be available for critical infrastructure protection.

The organizational approach to the implementation of Critical Infrastructure Protection in the European Union and the countries that strive towards full membership is given by the *Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (further Directive).[84]

The Introduction in the Directive clearly indicates how the primary and ultimate responsibility for protecting European critical infrastructures falls on the Member States and the owners/operators of such infrastructures.[85] This principle also applies to the protection of national critical infrastructures. From the aspect of cooperation between the public and private sectors, another provision of the Introduction of the Directive is very significant, which states how private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery, a Community approach needs to encourage full private sector involvement.[86]

The Directive also states how in organization of critical infrastructure protection it is necessary to have three important components: to make Operator security plans, assign Security Liaison Officers and nomination of critical infrastructure protection contact points. 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

[83] Myriam Dunn (2006) *Understanding Critical Information Infrastructures: An Elusive Quest* in: Myriam Dunn and Victor Mauer (eds.) INTERNATIONAL CIIP HANDBOOK 2006, VOL. II, Analyzing issues, Challenges, and Prospects, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf (cited 28 May 2017).

[84] 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 (cited 1 May 2017).

[85] Ibid, Introduction, paragraph 6.

[86] Ibid, Introduction, paragraph 8.

each Member State to decide on the most appropriate form of action with regard to the establishment of Operator security plans.[87] 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.[88] Effective protection of critical infrastructures requires communication, coordination, and cooperation at national and Community 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.[89]

Thereafter, a three-step process precedes the immediate implementation of critical infrastructure protection: 1.) Identification; 2.) Determination; 3) Protection. The identification of potential critical infrastructure is conducted by sectoral holders (competent ministries) in cooperation with regulatory agencies. Once when these stakeholders identify potential critical infrastructure within their own sector, they compile the list and submit it to the Government for confirmation. In the determination step, the Government looks at the proposed lists of potential critical infrastructures, and by decision determines individual critical infrastructure or all of the proposed. That decision is then delivered to the owner or manager of the critical infrastructure and to the relevant ministry and 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 level of protection of critical infrastructure. 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 the four basic principles of crisis management: prevention, preparedness, reaction and recovery. The mentioned plan must evaluate the analysis of the business risk of the critical infrastructure, its threats, the response strength, cooperation with the competent institutions, the implementation of protection measures, the scenario of the possible and worst possible event or more of them that can occur in the critical infrastructure. In addition, it must include a communication plan as well as the address book of the most important contacts.

Each country independently determines the organization and implementation of all processes and the level of involved actors within the Critical Infrastructure Protection System. There is no universal form to follow when establishing the system but there are certain above-mentioned principles that need to be respected to make the system more efficient, more cost-effective and self-sustainable. The private sector is an indisputable actor of these processes and of the system itself in all its parts.

[87] Ibid, Introduction, paragraph 11.

[88] Ibid, Introduction, paragraph 13.

[89] Ibid, Introduction, paragraph 17.

# 2. INSTITUTIONS COMPETENT FOR CRITICAL INFRASTRUCTURE PROTECTION

There are two basic approaches to the orientation of level of determining the critical infrastructure. The first approach is represented predominately by territorially smaller countries where the critical infrastructure is determined only at the national level and the other is present by larger countries where the critical infrastructure is determined from national, regional to local level. In the first case, the system is simpler for coordination because the relevant bodies of regional and local self-government units are not included in the processes as in the second case.

Since critical infrastructure represents a platform for maintaining the development of every society and state, it is appropriate that the level of involvement of institutions is also consistent with that. The Government of the state is involved in the critical infrastructure protection system as legislator to adopt laws and bylaws and to give power to individual ministries and/or central government bodies to be coordinators of the entire system and holders of sectoral processes. The Government delivers 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 (with special decision) the sectors from which central government bodies identify certain critical infrastructures in order to ensure a holistic approach to protecting and reducing negative impacts in case of threat to critical infrastructures.

Besides and following the Government, the next most important actor is the coordinator of the entire system of critical infrastructure protection. There are different examples and practices which body is appropriate for the named role. In the United States, this function is conducted by the Ministry of Homeland Security, in most European countries this function is assigned to the ministries of the interior. While there are examples such as 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 (independent central state level body below the ministries). There are many different solutions and practices, and it is for each country to recognize the most appropriate model. The system coordinator communicates directly with all system actors, international coordinators, submits reports to the Government and most often represents their own country at coordinative meetings organized by the European Commission. The mentioned institution, in cooperation with the competent central state administration bodies from whose scope the individual critical infrastructure is, regularly monitors, assesses the threats and proposes operational and other measures to assess the criticality and the need for the proposed measures for the management and protection of critical infrastructures.

Those responsible for the implementation of the sectoral policies are the central state administration bodies appointed by the Government (most commonly the relevant ministries). These institutions in cooperation with the competent regulatory agencies are responsible within their scope for identification (determination) of particular systems or their components as critical infrastructures, ensuring critical infrastructure management and their protection. As an example, we will take the energy sector. The competent institution is predominantly the Ministry of Economy (or the Ministry of Energy in individual countries), which delivers sectoral policies for the development of the relevant sector, cooperates, communicates and cares about the business of all actors in the market, carries out supervisory oversight, paying special attention to the area of sectoral critical infrastructure and their sectoral dependence and interdependence with other critical infrastructures from other sectors. There is a presumption, and what depends on state's development, 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 states have established Energetic regulatory agencies. These agencies have pubic authority and their activities are: issuance, extension and transfer of licenses for carrying out energy activities and temporary and permanent deprivation of permits; supervision of energy subjects in performing energy activities; supervising the management of business books; overseeing the principle of transpar-

ency, objectivity and impartiality in the work of the energy market operators; issuing a decision on acquiring the status of eligible energy producer and subtracting the said solution; 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 scope of competence of the central state administration body, in which collaborates the relevant ministry and regulatory agency (or more of them if they are present in the particular sector). Criteria for assessing the criticality of infrastructure can be: life and health - determining the impact of disruption and/or interruption of work on life and health; time frame - in case of disruption/interruption of work it will be determined in which time that disruption/interruption will have consequences on total business/service delivery (in 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 disruption of work; legal, regulatory and contractual significance; economic/financial damage.

Then the next actor is the owner or manager of the critical infrastructure. These are directly responsible for managing and protecting critical infrastructure under all conditions. They have 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. Alongside with law enforcement agencies, there is also a big role for companies which provide private security.

The challenge that is present everywhere in the world is to ensure the exchange of information, especially those which are sensitive so the owners/managers can have the cognition of whether they are endangered. The Directive 2008/114/EC itself, has recognized aforementioned and stated that critical infrastructure owners/operators should be given access to best practices and methods related to critical infrastructure protection, primarily through the relevant Member State bodies, and that the exchange of information should take place in an environment 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 demanding part of the critical infrastructure protection arrangement and an indicator of the general development of society and the state.

## 3. CRITICAL INFRASTRUCTURE PROTECTION PUBLIC-PRIVATE PARTNERSHIP

In the broad sense, a public-private partnership is often defined as a joint initiative of public and private sectors where each entity contributes to the system specific resources and participates in planning and decision-making.[90] That is exactly what should be aimed for in public-private partnership systems in the field of strengthening of resilience and critical infrastructure protection. The private sector in the western countries is the owner (manager) of more than 85 percent of national critical infrastructures, so it is understandable that the private sector is best familiar with critical infrastructure requirements – weaknesses and advantages, and it must be part of strengthening the resilience and protection of critical infrastructures. Awareness on importance of critical infrastructure protection for

90 For more information see: White House (1998) *Presidential Decision Directive/NSC-63,* Washington, https://www.fas.org/irp/offdocs/pdd/pdd-63.htm; 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; Heammerli, 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.

everyday functioning of all modern subjects, national security and international cooperation is rising, and exchange of knowledge, experiences and best practices between stakeholders (both private and public sector) for strengthening the resistance and protection of critical infrastructure system should be even common practice. We live in society where dependence on the regular functioning of critical infrastructure is part of our daily life, but unfortunately most citizens nor experts which are not involved directly in this and similar topics are not even aware of its existence. Due to these facts, it is necessary to invest more strongly in all segments of this key process.

Making appropriate system of critical infrastructure protection is very demanding task for any country at any degree of development. Threats are becoming more complex and endangering functioning of infrastructures which is very challenging for state, its bodies and operators. Generally, there are limited financial and organizational resources and critical infrastructure protection is usually one of last priorities for companies which manage critical infrastructures. Each state has its own approach to critical infrastructure protection, depending on degree of private ownership in the companies, soundness of state structure or past experiences. At the European level, it gets difficult to find and determine actions in the field of European critical infrastructure protection just because of that differentiation of approaches and specific of organization of states and legal order. For example, countries in Western Europe are more prone to market principles in securing protection of the critical infrastructure than Eastern and Southern European countries, which, because of the former socialist system, their organization of the protection of all important segments of the state and society have based on the role of the state. In this context, although in all the mentioned countries there has been a transition, a change in the structure and ways of carrying out a security activity, the state still represents a very important and central place for the regulation of relationships in terms of the authorities and responsibilities of the institutions for regulating individual social processes. Managing and ensuring the continuity of critical infrastructure certainly belongs among them. It will be needed for certain period to pass, before countries in Eastern and Southern Europe accept public-private partnership in protection of critical infrastructure in the full sense as indispensable and necessary concept of development and improvement of business and level of service.

Establishing a proper system of public-private partnership in the area of critical infrastructure protection is an ongoing process, which practically never ends. It is necessary to ensure the widest possible participation of proposals so it will be required, in addition to providing an appropriate level of awareness, to clearly define the authorities and responsibilities also at the level of critical infrastructure operators themselves. A significant part of an efficient system is mutual trust between stakeholders as well as exchange of information. There are usually two key categories of information: the information that is essentially important for ensuring national security and the information which in the business environment represents important business data, which may reduce the competitive advantage of the company that manages critical infrastructure. In particular it will come to the fore in the cases when ownership passes into private hands and several companies will appear in a certain area that will be in competition in the logic of the market economy. When it comes to companies that are in majority owned by the state, they are primarily focused on satisfying narrow political and economic goals, which are often not based on good governance and care for continuous operation of critical infrastructure. Also, private owners follow the main objective, which is reflected in the profit and investment in the maintenance and safe operation of critical infrastructure is not one of their important strategic objectives. All of these must be taken into account when we talk about building an effective critical infrastructure protection system. As one of the models of cooperation between the public and private sector and the need for exchange of information, we can point out the US example of Fusion Centers.[91]

[91] Department of the Homeland Security (2013) *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (cited 17 May 2017).

In public-private partnership it is necessary to focus also on certain elements for success and sustainability of cooperation for the purpose of implementing the objectives of resilience strengthening and protection of critical infrastructures, such as:

- Definition of roles and responsibilities – public-private partnership should regulate obligations and rights of public and private partners while respecting the basic principles in preparation and implementation of public private partnership projects, i.e. principle of public procurement, principle of public interest and principle of cost effectiveness.
- Application of resources – aimed at reduction of criticality and/or increased resilience of infrastructures, public private partnership stakeholders should involve resources available to them (e.g. capital), as already addressed by the national Public Private Partnership Act, and that should be a part of relevant contracts. In addition to the existing public and private financial resources, it is necessary to plan possible use of European structural and investment funds in support of public private partnerships in critical infrastructure protection.
- Openness for the development of capacities and changes – if the need for institutional changes arises in the process of critical infrastructures risk management at the level of the service provider or the government body.
- Realistic expectations – short term plans with limited timeframes result in solutions which are difficult to implement. More significant institutional changes which guarantee quality require time. Also, it is not realistic to expect that inclusion of the private sector over a short period of time shall compensate for shortcomings regarding resources or in activity of public institutions in general.[92]

## 4. PROGRAMS AND WORK PROCEDURES

Our opinion is that private sector has a one of the main roles in protecting critical infrastructure, based on public-private partnership and high levels of quality and service. Private sector needs to be recognized as a trusted partner by competent public authority and by owner/manager of critical infrastructure.

Although on EU level there is not yet a comprehensive set of measures to regulate critical infrastructure protection activities from private sector, jurisdiction is certainly in the domain of national legislation. On the other hand, there are ISO private security services sector specific safeguarding standards that need to be considered and implemented in the work of private sector before entering the critical infrastructure protection area. For example ISO 22300:2012 contains terms and definitions applicable to societal security to establish a common understanding so that consistent terms are used. ISO 28000:2007 specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain. ISO 18788:2015 provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the management of security operations. ISO/PAS 28007:2012, *Ships and marine technology – Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships.*

[92] EU funded project RECIPE (2015) *NATIONAL STANDPOINTS Project - Resilience of Critical Infrastructure Protection in Europe (RECIPE)*, www.recipe2015.eu, (cited 23 May 2017).

Besides that, there is another very high quality document to which needs to draw attention of private sector, but also of public institutions and critical infrastructure owners. It is the manual "Buying quality private security services", developed by the Confederation of European Security Services (CoESS) and UNI - Europa with the financial support of the European Union.[93] This manual tries to provide the buyer with the necessary arguments for which private security services should be based on best value, including social criteria relevant to the sector. It shows the key importance of defining, identifying, searching and selecting best value for private security services. The manual covers, in this sense, all aspects of a tendering process. It assists buyers with defining what they consider as quality; drawing up tender documents where those quality elements are reflected; comparing tender submissions with the practical tool developed as part of this manual where different bids can be evaluated against the originally selected quality criteria; and finally evaluation of the bids using the selected quality criteria, and selection of the bid with the highest quality up to the signature of the contract.

The protection of critical infrastructure by the private sector is an activity that includes the protection of objects and various forms of property which is done with physical and/or technical protection. Private security may be provided by persons and companies that have granted permission by the police administration to carry out these tasks. The basic function of protecting the critical infrastructure by the private sector is preventive action. Private protection represents the most massive and most expert form of organization of society and individuals in a self-defense and preventive sense. The private sector provides services and carries out protection tasks that cover those areas that are not secured by the competent state bodies or it is a complement to security activities performed by state bodies.

**Physical protection** is defined as the immediate guarding and securing of objects and various forms of critical infrastructure assets. According to the UN when considering the physical protection of critical infrastructure from the terrorist threats, mentioned means a complex process that needs to encompass the entire cycle of a possible terrorist attack. It requires cooperation domestically and across borders. The physical protection of critical infrastructure can prevent the commission of high-impact terrorist attacks. Inevitably, some terrorist plots will succeed. The immediate response may prevent the "cascading" effects that such attacks frequently entail, including further victims.[94] It is important to perceive and understand how in protection of critical infrastructure, absolute security does not exist. This should not be used as an alibi and a pre-set justification, but as an understanding of the complexity of the tasks which are needed to be done and the constant need to upgrade the protection system.

**Technical protection** is a set of actions that directly or indirectly protect the critical infrastructure. It is carried out with technical means and devices and systems with the primary purpose of preventing unlawful actions directed towards critical infrastructure. By that, the most commonly applied measures in technical protection are: anti-theft and counterfeit techniques; protection against unauthorized access to protected areas; protection against the carrying explosive, ionizing and other dangerous substances into objects; protection against the removal or the alienation of protected objects.

Technical protection is carried out in the area of the protected object or in the protected premises itself. Technical means and devices can be connected to technical protection systems. Systems of technical protection should be implemented, maintained and serviced in accordance with the regulations on the conditions and the manner of implementation of technical protection. Means and devices for technical protection are means and devices for the physical prevention of unauthorized entry of persons into a protected object, some of which are: special fences; special ramps and barricades; anti-

[93] Confederation of European Security Services (CoESS) and UNI - Europa (2014) *Buying quality private security services*, http://www.securebestvalue.org/wp-content/uploads/2014/11/Best-Value-Manual_Final.pdf (cited 13 May 2017).

[94] 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, page 11 (cited 2 June 2017).

theft doors; all types of locks with serial number or code; special building construction; impenetrable glass and similar constructions; equipment for storage, preservation and transfer of values objects and documents (cash registers, safes, security containers, etc.); detection devices for metal objects; X-ray devices for baggage control.

With technical protection, such as sensory and alarm systems and video surveillance, security guards increase the safety of objects, persons and property. Security systems can be connected to dispatch centers, which receive direct information about the possible burglary and send the mobile security team to the place of happening.

# 6 CHAPTER CRITICAL INFRASTRUCTURE PROTECTION IN THE REPUBLIC OF MACEDONIA

After its independence, the Republic of 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 foreign policy principles, as well as security policy principles within that framework, as an inseparable part in realization of own national interests. Within the most important activities, on which security policy further adds up, also falls critical infrastructure protection.

The most important activities, on which critical infrastructure protection is further integrated, include:

- 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 Macedonia is not in accordance with the guidelines of the European Union. In that direction, there is a lack of clear specification of the critical infrastructure term. Therefore, it is generally accepted that in specification of the objects as critical infrastructure, one should start from the analysis of several decisions, namely:

- 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 Macedonia, such as: electricity, postal and shipping, railways, airports, water supply, etc.
- Decision on determining the legal entities that are obliged to have private security.[95] The Decision specifies the provision of legal entities, whose activity is related to handling, as following:
  - 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 carriage of dangerous goods;
  - legal entities registered for handling objects and facilities of particular cultural and historical significance.[96]

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

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

[96] 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

activities have been defined, namely:

- ❖ energy (production, transmission and distribution of energy);
- ❖ water supply;
- ❖ environment;
- ❖ Macedonian Radio and Television, electronic and print media;
- ❖ National Bank of the Republic of Macedonia and other legal entities registered for carrying out banking activities.[97]

## 1. PROTECTION AND SECURITY OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF MACEDONIA

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

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

*The Energy sector* in the Republic of Macedonia is regulated in accordance with the Energy Law. Here, as priority, we would highlight strategically the most important companies, such as: "JSC ELEM" (Macedonian Electric Power Plants) and "JSC MEPSO" (Electricity Transmission System Operator of Macedonia), which together with their capacities represent the pivot 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 derivates in the Republic of Macedonia.

*Information technologies.* In this sector, special emphasis should be placed on the wide range of measures for critical infrastructure security and protection. As priorities, we would highlight 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 fixed and mobile network and the most sophisticated information technologies.

*Water systems* in the Republic of Macedonia are regulated in accordance with the Law on Water. 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 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;

[97] Ibid

- Ministry of the Interior;
- Airport operators; and
- Air carriers.[98]

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, one 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, airlines, 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 an Airport Safety Committee;
- other efficient bodies with which policy and standards for implementation of security measures would be coordinated.[99]

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

[99] Alcheski Gj., (2016), Implementacija na sovremenite bezbednosni sistemi i proceduri vo razvojot na obezbeduvanjeto na objektite od vitalen interes za Republika Makedonija (so osvrt na aerodromskata bezbednost), Filozofski fakultet, Skopje, pp.213-214

# 7 CHAPTER EXAMPLES OF PAST TERRORIST ATTACKS ON CRITICAL INFRASTRUCTURE

The new era of terrorism began with the terrorist attacks in the United States, continued with the terrorist attacks in Madrid, London, Brussels, Paris, Manchester and elsewhere. According to experts' assessments, the previous warfare tactics the so-called "modus operandi" of Al-Qaeda has been changed. Novelty is the new direction of "target's choice". Regardless the motives for this change, it is important to emphasize that the goal is aimed at destroying certain parts of critical infrastructure or the so-called "soft targets" and inflict a major blow.

A confirmation of this is the terrorist attack in the United States, when on September 11, 2001, Al-Qaeda members hijacked 4 commercial aircrafts, diverting their flights to specific targets: the World Trade Center and the Pentagon. This will be followed by the fact that the death toll at the World Trade Center amounted 2.603, while the number of passengers killed in the four aircrafts was 246. In the Pentagon building 125 were killed, another 24 went missing and are believed to have been killed.[100]

According to the estimates of the US experts, 16.000 people were in the World Trade Center's danger zone at the time of the attacks. Hence, the positive contribution was primarily to provide conditions for timely evacuation to 92% of them. Of course, it is of particular importance that this percentage of evacuated citizens affected the balance of the dead to be smaller.

At the same time, the terrorist attacks in New York, apart from many casualties, caused a decline in the economy as well. According to the data, GDP growth was low, that is the fall in the economy led to a complete recession.[101]

Bearing in mind the general knowledge of the analysis of the terrorist attack, one can conclude that the subsequent analyses were directed towards:

- the challenges facing civilians and the private sector;
- the omissions from the lack of a rescue protocol from the top of a building;
- the fire protection plan;
- the 911 service; and
- the readiness of civilians for protection during such terrorist attacks.[102]

In fact, the terrorist attacks have demonstrated the absence of an effective government approach to assessing weaknesses and readiness to cope with terrorist attack and critical infrastructure protection.

Namely, these terrorist attacks have influenced rapid changes, such as:

First, in October 2001, the "Patriot Act" was drafted.

Second, a revision was made to the Directive on Critical Infrastructure Protection in the US, issued in May 1998.

Third, a Directive on Critical Infrastructure Identification, Prioritization and Protection was drafted, and it was adopted in June 2004.

[100] Commission Report, 9/11, http://govinfo.library.unt.edu/9/11/report

[101] A Retrospective Assesment, Congressional Research Service: The Ekonomic Effects of 9/11

[102] For this aspects see Commission Report 9/11

Fourth, a National Plan for Critical Infrastructure Protection was adopted in 2006.

Fifth, the Federal Emergency Management Agency (FEMA) has undergone changes and has become part of the Homeland Security Department (Emergency Preparedness and Response Directorate).

On 11 March, 2004, a new terrorist attack on critical infrastructure was carried out in Madrid, Spain. According to statements by official authorities, these attacks were carried out by ETA and Al-Qaeda.

These terrorist attacks were carried out in a series, as follows:

- Atocha station – two trains were blown;
- El Pozo station – one train was blown; and
- Santa Eugenia station – one train was blown.

According to the government's investigation, it was proven that they were not suicide attacks but controlled attacks with remote explosive devices.

In particular, the death toll was 192, while the number of injured was 1.800, which, in turn caused great deal of fear, shock, and disbelief, primarily because of the controversy over the real culprits.

On 7 July 2005 a new terrorist attack on critical infrastructure was carried out in London, United Kingdom.

These terrorist attacks were carried out in three underground trains and one double-decker bus. The death toll was 56, of which 4 suicide bombers and 700 injured.

According to British experts, sophisticated means were used in terrorist attacks in London, and explosive devices were activated via a mobile phone alarm, in order to trigger explosives in the biggest traffic jams and thus cause maximum casualties.[103]

The terrorist methods and targets of the London attack should be analyzed in several respects.

According to the first standpoint, the planning and execution of the four simultaneous attacks are key evidence of future novel trends, that is, new "soft targets" in terrorism.

According to the second point of view, the tactics of suicide attacks on simultaneous multiple attacks have added additional difficulties in terms of time, space and resources, in the phase of prevention, coping and post-terrorist response phase.

According to the third standpoint, terrorist attacks on critical infrastructure are exclusively aimed at achieving a shocking psychological effect with numerous civilian casualties.

From the terrorist attacks on critical infrastructure in recent years, we would single out the terrorist attacks in Paris, Brussels, and Manchester. On 13 and 14 November 2015 a terrorist attack was carried out in six locations in the center of Paris, France with 129 people killed and 300 injured. On 22 March 2016, a terrorist attack on critical infrastructure was carried out in Brussels, Belgium. These terrorist attacks were carried out at the Belgian airport, by triggering two explosions. The death toll was 31 dead and 250 injured. On 23 May 2017 at "Manchester Arena" and the nearby railway station in Manchester, United Kingdom, two terrorist attacks were carried out and the death toll was 19 dead and 59 injured.

The conclusion from the analysis of some of the past terrorist attacks on the critical infrastructure can serve as an example of the starting point in creating changes it the approach to protect it. The new era of terrorism, the new warfare tactics with a clear goal aimed at destruction of critical infrastructure, that is, "soft targets", also require a new approach to critical infrastructure protection. Therefore, we will set several priorities, namely:

- creating effective strategy for critical infrastructure protection;

[103] US Army Tradoc G2 (2007) Terror Operations: Case Studies in Terrorism, Kansas, pp.91-92

- applying multiple early warning models;
- successful prevention, which can contribute to risk reduction, which will directly affect the increase in the safety of critical infrastructure;
- continuous training of human resources to deal with critical infrastructure attacks;
- updating or adoption of Law on Critical Infrastructure Protection, National Program for Critical Infrastructure Protection, National Plan for Critical Infrastructure Protection, and other documents directly or indirectly related to critical infrastructure protection.

# LITERATURE


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

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

**Birkett, D.M.,** (2017) Water Critical Infrastructure Security and Its Dependencies. Journal of Terrorism Research. 8(2), pp.1–21. DOI: http://doi.org/10.15664/jtr.1289 .

***Bognar, B.,*** (2009), The process of critical infrastructure protection, AARMS, Budapest.

***Brömmelhörster, Jörn; Fabry, Sandra and Wirtz, Nico*** (2004) *Critical Infrastructure* Birkett, D.M. (2017) Water Critical Infrastructure Security and Its Dependencies. Journal o *Protection: Survey of World-Wide Activities*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.html.

***Davidović, D., Kešetović, Ž. Pavičević, O.,*** (2012), *National Critical Infrastructure Protection in Serbia: The Role of Private Security,* Journal of Physical Security; 6(1), 59-72, Argonne National Laboratory, http://jps.anl.gov/Volume6_iss1/Davidovic.pdf.

***DCSINT Handbook,*** (2006), Critical infrastructure threats and terrorism, Kansas, No.1.02, p. 1

Commission of the EU,( 2004).

***Dunn, Myriam*** (2006) *Understanding Critical Information Infrastructures: An Elusive Quest* in: Myriam Dunn and Victor Mauer (eds.) INTERNATIONAL CIIP HANDBOOK 2006*,* VOL. II, Analyzing issues, Challenges, and Prospects, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2.pdf.

***Heammerli, 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.

***Keković, Z.,*** (2013), National Critical Infrastructure protection regional perspective, Belgrade.

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

***Levis, G.,*** (2006), Critical Infrastructure in Homeland Security-Defending a Net-worked National, John Wiley & Sons Inc. Hoboken, New Jersey (USA).

***Lee, E.,*** (2009) *Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection*, Boca Raton, Taylor & Francis Group: Auerbach Publication.

***Leuven, Van and Laurie,*** (2011) *Water/Wastewater Infrastructure Security: Threats and Vulnerabilities*, https://www.researchgate.net/publication/226050430_WaterWastewater_Infrastructure_Security_Threats_and_Vulnerabilities.

***Luiijf, Eric and Klaver, Marieke*** (2015) *Governing Critical ICT: Elements that Require Attention*, http://societalsecurity.net/sites/default/files/document-database/files/2016-03/pdf/3018787-governing-critical-ict-elements-require-attention.pdf.

***Marjanović, M. and Nađ, I.*** (2013) National critical infrastructure protection –regional perspective: Assessment of threats to critical infrastructure facilities from serious and organized crime, Belgrade.

***Perinić, J. and Mikac, R.,*** (2014) *Protection of the critical infrastructure from terrorism: Case study of the Republic of Croatia*, in: Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection, NATO Science for Peace and Security Series: Information and Communication Security.

***Prezelj., I.,*** (2008) Konceptualna opredelitev kritične infrastructure, Fakultet društvene vede, Ljubljana.

***Theoharidou, Marianthi; Kandias, Miltiadis and Gritzalis, Dimitris*** (2012) *Securing Transportation-Critical Infrastructures: Trends and Perspectives*, https://pdfs.semanticscholar.org/5441/f94eb1dbb98f9fa4031c52ef3e476f71050b.pdf .

*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.**

## REPORTS AND DIRECTIVES

***A Retrospective Assessment,*** Congressional Research Service: The Economic Effects of 9/11

Commission Report 9/11.

***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.

***Canadian Security Intelligence Service*** (2017) *Cybersecurity and Critical Infrastructure Protection*, https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php, (cited 12 June 2017).

***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.

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

***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.

***Confederation of European Security Services*** (CoESS) and UNI - Europa (2014) *Buying quality private security services*, http://www.securebestvalue.org/wp-content/uploads/2014/11/Best-Value-Manual_Final.pdf.

***Commission Report,*** 9/11, http://govinfo.library.unt.edu/9/11/report.

***Department of the Homeland Security*** (2007) *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, https://www.hsdl.org/?view&did=474328.

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

***European Union Council Directive*** (2008), On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, 23/12/2008.

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

***European Commission*** (2005)*Green Paper on the European program of Critical Infrastructure Protection,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005DC0576.

***European Commission*** (2006) *European program of Critical Infrastructure Protection,*http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786.

***European Commission (***2012) *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

***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*, https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf.

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

***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.

***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.

***EU funded project RECIPE*** (2015) *NATIONAL STANDPOINTS Project - Resilience of Critical Infrastructure Protection in Europe (RECIPE)*, www.recipe2015.eu.

***FOCUS D5, (***2012), Problem space report: Critical Infrastructure & Supply Chain Protection, Cross Border Research Association (CBRA).

***Green paper on a European Programme*** for critical infrastructure protection, (2005), Brussels, Annex II.

***Government of the Republic of Croatia*** (2009) *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća*, http://www.duzs.hr/download.aspx?f=dokumenti/Stranice/PROCJENAUGROZENOSTIREPUBLIKEHRVATSKE.pdf.

***Home Office*** (2009), *National Counterterrorism Strategy*, *Government of the United Kingdom,* http://tna.europarchive.org/20100419081706/http:/security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy-2009?view=Binary.

***International Atomic Energy Agency*** webpage, http://www-pub.iaea.org/books/IAEA-Books/Publications_on_Accident_Response.

***Ministry of Interior*** (2011) *Regulation for the Protection of Critical Infrastructure*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf.

***National Strategy for Critical Infrastructure Protection*** (CIP Strategy) of Federal Republic of Germany, 2013

***NATO Parliamentary Assembly*** (2008) *Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures,* **http://www.nato-pa.int/Default.asp?SHORTCUT=1478**.

***Office of Homeland Security*** (2002), *National Strategy for Homeland Security*, https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf .

***Presidential Policy Directive***, (2013) Critical Infrastructure Security and Resilience The White House Office of the Press Secretary, USA.

***Public Safety and Emergency Preparedness Canada*** (2003) *Water, Critical Infrastructure Protection and Emergency Management*, http://publications.gc.ca/collections/collection_2008/ps-sp/PS4-7-2004E.pdf.

***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.

***Spanish Parliament (***2011) *Law 8/2011 by which measures for the Protection of Critical Infrastructure Protection*, http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf.

***TIME (***2009) *The Worst Nuclear Disaster*, http://content.time.com/time/photogallery/0,29307,1887705,00.html.

***US Army Tradoc G2 (***2007) Terror Operations: Case Studies in Terrorism, Kansas.

***United States Congress*** (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA PATRIOT Act),*стр.401, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

***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.

***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.

***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.

***White House*** (1998) *Presidential Decision Directive/NSC-63,* Washington, https://www.fas.org/irp/offdocs/pdd/pdd-63.htm; 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;

## LAWS AND BYLAWS

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

Law on Private Security, "Official Gazette of the Republic of Macedonia", Skopje, no.166/2012

Law on Amending and Supplementing the Law on Private Security, "Official Gazette of the Republic of Macedonia", Skopje, no.164/2013

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