CRITICAL INFRASTRUCTURE – IDENTIFICATION AND PROTECTION

Teodora Gechkova*

Introduction

Critical Infrastructure

"[A]n asset, system or part thereof located in member states that 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 on a member state as a result of the failure to maintain those functions." [1].

Table 1: Selected Countries and their definitions of Critical Infrastructure

Country	Definition
United States	Critical infrastructure describes the physical and cyber systems and assets that are ~~so~~ vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society [2].
Canada	Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of the government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence [3].
Germany	Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences [4].

* Teodora Gechkova, Chief. Assist. Prof. PhD, Department of National and Regional Security, UNWE, email: tgechkova@unwe.bg

Czech Republic	The basic function of the government is to ensure the protection and development of the protected interests and sustainable development of human society. The Constitution of ~~the~~ Czech Republic, as the highest legal document of the Czech Republic, declares that the protected interests of the state are the goals that are cherished as a priority, i.e. the lives and health of people, property, the environment, and safety [5].
Bulgaria	"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"[6].

European Critical Infrastructure

"European critical infrastructure" or 'ECI' 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" [7].

Table 2: European Critical Infrastructure – Sectors

Sector	**Subsector**
Energy	Electricity – Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity; Oil – Oil production, refining, treatment, storage and transmission by pipelines; Gas – Gas production, refining, treatment, storage and transmission by pipelines ; LNG terminals
Transport	Road transport; Rail transport; Air transport; Inland waterways transport; Ocean and short-sea shipping and ports.

Source: Council Directive 2008/114/EC

Protection

"Protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralize a threat, risk or vulnerability" [8].

Main threats and risks for critical infrastructure

Risk – "The risks are increasingly complex and frequent. They include natural, intentional and accidental hazards" [9].

Threat – in the field of critical infrastructure protection, there are five categories of threats:

- natural disasters;
- technological accidents;
- cyber-attacks;
- criminal activities;
- terrorist attacks;

Natural disasters "can have a significant impact on CI elements in a short period of time. The primary point of impact tends to be the physical infrastructure, such as hydro lines and bridges. Damage is not always localized, often resulting in a ripple effect across a number of sectors." [10].

Technological accidents "represent incidents in which there is a negative effect on functionality, structure and integrity of the system due to internal factors (reliability mainly). The internal factors may be faults, failures and other unreliability, causing uncontrolled degradation and destruction of functions. Protection of critical infrastructure element is provided by ensuring of technology reliability." [11].

Cyber – attack "The threat is not restricted by political or geographical boundaries. Attacks can originate from anywhere in the world and from multiple locations simultaneously. Investigations and back tracking through a web of false leads and unwittingly slaved systems can be time consuming and resource intensive to pursue." [12]. Protection is provided by cryptography and reliable secure communication protocols.

Criminal activity "Any damage or interruption causes ripples across the system. Attacking infrastructure, therefore, has a "force multiplier" effect, allowing a small attack to achieve a much greater impact." [13]. Protecting of critical infrastructure elements is a summary of measure of physical security.

A terrorist attack is usually " [14] illegal activities leading to the degradation or destruction of critical infrastructure elements to support the enforcement of its policy goals. Protecting critical infrastructure elements is a summary of measure of physical security."

Critical Infrastructure Protection: Main players (Canadian experience)

Table 3: Roles and Responsibilities in Canadian Critical Infrastructure Protection

	Roles	Responsibilities
Federal Government	Lead federal activities	Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure; Collaborate with provincial and territorial governments to achieve the objectives of the Strategy; Collaborate with national associations; Collaborate with critical infrastructure owners and operators within federal mandate in consultation with provinces and territories;
Provincial/territorial governments	Lead provincial/ territorial activities	Advance a collaborative federal, provincial and territorial approach to strengthening the resiliency of critical infrastructure; Collaborate with federal, provincial and territorial governments to achieve the objectives of the Strategy; Coordinate activities with their stakeholders, including municipalities or local governments where it applies, associations and critical infrastructure owners and operators.
Critical infrastructure owners/ operators	Collaboratively manage risks related to their critical infrastructure	Manage risks to their own critical infrastructure; Participate in critical infrastructure identification, assessment, prevention, mitigation, preparedness, response and recovery activities.

Source: Action Plan for Critical Infrastructure

Measures for critical infrastructure protection

1. Risk analysis and crisis management
2. "risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure" [15];
3. "This risk management approach is based on a philosophy of continuous improvement, which involves setting protection and resiliency goals, identifying critical infrastructure and key dependencies, assessing and prioritizing risks, developing and executing plans and programs to address the

identified risks and dependencies, and measuring the effectiveness of the plans and program" [16].

4. Business continuity planning;
5. "Can be defined as an effort within sectors or elements of critical infrastructure, aimed to ensure that critical functions keep their operational status, during a wide range of emergencies, including localized acts of nature, accidents, technological or attack-related emergencies" [17];
6. IT security;
7. "Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks" [18]. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become a very important government security mission;
8. Physical protection;
9. "In critical infrastructure protection the physical protection of any object (building, appliance, object etc.) is achieved by combining and intertwining of three basic elements: physical protection systems, response team/ activity, regime protection." [19].

Procedure of Identification of Critical Infrastructure in Bulgaria

A procedure of identification of national critical infrastructure (sectors, objects and elements) consists four main steps:

Definition of critical infrastructure

The definition of critical infrastructure is s result of European legislation (directives) and national framework, which reflected national interests

Selection of critical infrastructures within individual sector

The process of identification of national critical infrastructure in Bulgaria started in 2009, when Ministries and other central administrative authorities, defined strategic objects, which are with strategic importance for national security of the country.

In 2012 were defined sectors and objects in national critical infrastructure.

Definition of European critical infrastructure

In Bulgaria European Critical Infrastructure was defined in 2008 in answer of European Commission's requirements.

This step is carried out by the same entities as in the previous two steps.

Cross-cutting criteria

- casualty's criterion (assessed in terms of the potential number of fatalities or injuries);

- economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
- public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services)

A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be a European Critical Infrastructure

Conclusion

Critical infrastructure is a very complex system, which reflected national interests of each country. It contains sectors, objects and elements, protection of them is a task for governments, ministries, administrative authorities and public and private sector. The risks and threats for critical infrastructure are unpredictable (terrorism, cyber- attacks and some natural disasters). The programs, mechanisms and measures for protection are very important for national security.

Notes

[1] European Council Directive 2008/114/CE.
[2] Infrastructure Security – https://www.dhs.gov/topic/critical-infrastructure-security
[3] National Strategy for Critical Infrastructure – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
[4] National Strategy for Critical Infrastructure Protection (CIP Strategy) in Germany
[5] Michaela Vašková, Protection of the Object of the Critical Infrastructure in the Czech Republic, World Academy of Science, Engineering and Technology International Journal of Economics and Management Engineering Vol:9, No:12, 2015
[6] Republic of Bulgaria, Ministry of Energy – https://www.me.government.bg/en/themes/critical-infrastructure-in-the-energy-sector-336-300.html
[7] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[8] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[9] National Strategy for Critical Infrastructure in Canada – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

[10] Threats to Canada's Critical Infrastructure – https://www.publicsafety.gc.ca/lbrr/archives/cn000034012674-eng.pdf
[11] Lukas, L., Hromada., M., Management of Protection of Czech Republic Critical Infrastructure Elements, Recent Searches in Automatic Control. P, 307
[12] Threats to Canada's Critical Infrastructure – https://www.publicsafety.gc.ca/lbrr/archives/cn000034012674-eng.pdf
[13] Threats to Canada's Critical Infrastructure – https://www.publicsafety.gc.ca/lbrr/archives/cn000034012674-eng.pdf
[14] Lukas, L., Hromada., M., Management of Protection of Czech Republic Critical Infrastructure Elements, Recent Searches in Automatic Control. P, 307
[15] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[16] Canada – United States Action Plan for Critical Infrastructure – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx
[17] Giacchero, A., Giordano, F., M. Schiraldi, M., From business continuity to design of critical infrastructures: ensuring the proper resilience level to datacenters, International Journal of Engineering and Technology • August 2013
[18] Homeland Security – https://www.dhs.gov/cisa/cybersecurity
[19] Ludek, L., Necesal, L., Measures for Critical infrastructure protection, International Journal of Mathematical Models and Methods in Applied Sciences, p. 1254

References:

Action Plan for Critical Infrastructure – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/pln-crtcl-nfrstrctr-eng.pdf
Canada – United States Action Plan for Critical Infrastructure – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx
Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
Giacchero, A., Giordano, F., M. Schiraldi, M. (2013), From business continuity to design of critical infrastructures: ensuring the proper resilience level to datacenters, International Journal of Engineering and Technology
Homeland Security – https://www.dhs.gov/cisa/cybersecurity
Infrastructure Security – https://www.dhs.gov/topic/critical-infrastructure-security
Ludek, L., Necesal, L., Measures for Critical infrastructure protection, International Journal of Mathematical Models and Methods in Applied Sciences, p. 1254
Lukas, L., Hromada., M., Management of Protection of Czech Republic Critical Infrastructure Elements, Recent Searches in Automatic Control, p, 307.

Michaela Vašková (2015), Protection of the Object of the Critical Infrastructure in the Czech Republic, World Academy of Science, Engineering and Technology International Journal of Economics and Management Engineering Vol:9, No:12,
National Strategy for Critical Infrastructure – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
National Strategy for Critical Infrastructure in Canada – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
National Strategy for Critical Infrastructure Protection (CIP Strategy) in Germany
Republic of Bulgaria, Ministry of Energy – https://www.me.government.bg/en/themes/critical-infrastructure-in-the-energy-sector-336-300.html
Threats to Canada's Critical Infrastructure – https://www.publicsafety.gc.ca/lbrr/archives/cn000034012674-eng.pdf

CRITICAL INFRASTRUCTURE – IDENTIFICATION AND PROTECTION

Abstract

The article considers the EU as a region, part of which also is Bulgaria. It analyzes the critical infrastructure in the US and Canada. In the research has been suggested a procedure for identifying the national critical infrastructure, similar to the method of Czech Republic. The article has been proposed main measures for the protection of national critical infrastructure and analyzed major definitions like: risk, threat; Critical Infrastructure; European Critical Infrastructure, etc.

Key words: critical infrastructure; protection; strategic planning; measures; physical protection

JEL: O18