CRITICAL INFRASTRUCTURE PROTECTION WITHIN THE EUROPEAN UNION

Vasile POPA

Professor, Ph.D, Transylvania University, Brasov, Romania

The new dynamics and intensity of the risks and threats posed to societal functioning and citizens' security have acquired new meanings. Consequently, an integrated approach to the concept of "critical infrastructure" is necessary. The critical nature of some of the basic characteristics of the critical infrastructures has made them acquire new meanings within the national/transnational strategic planning. Moreover, the complexity and importance of critical infrastructure protection for social stability have generated the correlaton of the strategies developed by states and organizations.

Key words: *critical infrastructure, vulnerability, risk, threat, critical infrastructure protection*

1. INTRODUCTION

The swift and highly unpredicatble changes in nowadays world, coupled with the complexity of vulnerabilities and risks lead to a major concern regarding the protection of the critical infrastructures. The transnational links among these enabled by the globalization process and the extended risks to which they are prone make it possible for any aggression against a state, a system or a process to generate a cascade effect. Consequently, the globalization of insecurity should be countered by a globalization of security measures and systems in order to better cope with current and future threats.

The new dynamics and intensity of the risks and threats posed to societal functioning and citizens' security have acquired new meanings. Consequently, an integrated approach to the concept of "critical infrastructure" is necessary. The critical nature of some of the basic characteristics of the critical infrastructures has made them acquire new meanings within the national/ transnational strategic planning. Moreover, the complexity and importance of critical infrastructure protection for social stability have generated the correlaton of the strategies developed by states and organizations.

The past few years characterized by terrorist attacks, by deliberate energetic supplies cutouts at state level, by technological accidents triggered by human mistaks or by natural disasters have revealed the vulnerability of national critical infrastructures. in this respect, the EU member states have taken firm action towards identifying a joint

approach to the protection of their strategic objectives.

The terrorist attacks of 2011 in the USA, of March 2004 nin Madrid and of July 2005 in London, the economic crisis, the global spread of diseases and the energetic problems have revealed the vulnerability of modern societies to asymmetric threats. As a result, national interest and the adoption of measures towards identifying and protectin critical infrastructures have become of prime importance. The state that coined the phrase of critical infrastructure in 1995 and took the first steps in this direction was the USA by establishing a Critical Infrastructure Committee to deal with border security and the prevention of attacks from outside. Important legal and institutional initiatives in the definition of critical infrastructurees were also developed aby NATO and by EU member states. In this respect, at NATO level, the Senior Civil Emergency Planning Committtee was established to find and identify integrated strategies to analuze and protect critical infrastructures. At the EU level, especially after the 2004 and 2005 terrorist attacks in Madrid and London, a set of measures was adopted in oredr to shape the legal and operational framework needed to protect critical infrastructures.

2. THE CONCEPT OF CRITICAL INFRASTRUCTURE AT EU LEVEL

2.1. Definitions [1]

According to the National doctrine on security information [2], the concepts of "vulnerability", "risk factors", "threats", "danger", "aggression" are defined from the perspective of the overall concept of "critical infrastructure" as follows:

Vulnerabilities – processses, phenomena that diminish the reaction capacity of the critical infrastructures to existing or potential risks, or that favor their emergence and development with consequences for their functionality and usefulness. The mismanagement or lack of knowledge can generate risk factors, threats or dangers to national goals, values, interests and necessities, all of which are considered critical infrastructures.

Risk factors – refer to all circumstances, both internal and external, that favor the emergence of a threat to critical infrastructures due to a gven vulnerability and with direct effects at security level.

Threats – are the capacities, strategies, intentions, plans that contribute to the increase of threats to critical infrastructures. They may be in the form of attitudes, gestures, deeds that lead to imbalance or instability and generate danger impacting national security.

Threat state – is a situation that appears and threatens the existence and integirty of critical infrastructures.

Aggressions – are the attacks, the armed ones included, that endanger the existence, balance or equilibrum of critical infrastructures.

National Critical Infrastructure (NCI)– an element, system or system component that is to be found at national level and that is essential in ensuring the vital functions of a society, as well as the health, security, social or economic welfare of people and whose disruptiion can significantly impact a nations' stability.

European Critical Infrastructure (ECI) - a national critical infrastructure whose disruption would siginficantly impact at least two EU member states. The seriousness of the impact is evaluated based on the dependecies between the given infarcstructure and others and the extent of the damage brought to all of these.

Critical Infrastructure Protection (CIP) - is aimed at ensuring the functioning, continuity and integrity of NCI/ECI by descouraging, diminishing or neutralizing a threat, risk or vulnerability. The CIP refers to the activities concerned with risk analysis and evaluatin, classified information protection, security planning on behalf of those who operate the critical infrastructures, etsablishing the liaison officers and the communication means, as well as drills, reports, reevaluations and documentation updates.

Risk analysis - is the analysis of the scenarios concerning the emergence of critical threats undertaken in order to identify the likely impact of a critical infrastructure's disruption or destruction.

Critical infrastructure sensitive information - is the information concerning a critical infrastructure that could be used, in case of revealing, to disrupt or destroy the elements of a critical infrastructure.

Owners/operators of a European critical infrastructure (OECI)- are the entities in charge with making investments in a given element, system or component of a critical infrastructure.

2.2. Critical infrastructures defined by specialised litereature

Specialised literature identifies three types of critical infarstructures depending on their importance to the stability of the economic and social security systems:

- **Regular infrastructures** that provide the framework for the establishment and functioning of a system;
- **Special infrastructures**, with a role in ensuring the functioning of systems and processes and with a high impact on the overall stability and security of the socio-economic systems at regional level. Once subjected to vulnerabilites or dysfunctions, as well as under the influence of insecurity they can become critical.
- **Critical infrastrutures** have a major role in the stability, security and safety of systems and processes unfolded at economic, social, political and military level. Their critical nature is the result of the effects their disruption, even temporary, may yield at national or global level [3]. An infrastructure or set of infrastructures can be considered critical if:
- It has a unique status within a process or system or and it is tightly knit to the other infrastructures within the latter;
- It plays an important role in the stability, feasibility, safety, functioning and security of systems;
- It is exposed to direct threats and, hence, represent a vulnerability within the systems or processes it is part of;
- It is highly influenced by the changes in the environment [4].

2.3. The development of the critical infrastructure concept witihin the EU (2004 – 2008)

2.3.1. A global strategy for Critical Infrastructure Protection

The multifarious effects of the terrorist attacks in the USA (2001),

Madrid and London on the critical infrastructures of nations and of alliances revealed their vulnerabilities. Consequently, in June 2004, the EU Council asked the EU Commission to prepare a global strategy for Critical Infrastructure Protection. In October 20 2004, the latter adopted a set of communiqués concerning the topic: *Prevention, preparedness and response in terrorist attacks, COM (2004) 698; Prevention of the Fight against Terrorist Financing, COM (2004) 700; Preparedness and consequence management in the fight against terrorism, COM(2004) 701;* Critical Infrastructure Protection in the fight against terrorism, COM (2004)702.

2.3.2. The Critical Infrastructure Warning Information Network - CIWIN

In 2005, the European Commission established the CIWIN. Ist role is to provide the specialists in CIP within the EU to contribute to the creation of a program that allows information exchange at EU level concerning common threats and vulnerabilites, as well as the development of an appropriate countering startegy. The USA counterpart is known by the name of **Critical Infrastructure Warning Information Network (CWIN)**.

2.3.3. The European Programme for Critical Infrastructure Protection (EPCIP)

In November 17 2005, the Commission adopted the *Green Paper* that concerns the etsablishment of a European Programme for Critical Infrastructure Protection through public debate and discussion with the operators of the critical infrastructures identified in the EU documents, as well as the founding of a Critical Infrastructure Warning Information Network (CIWIN). The elements that were brought to the attention of the EU members were as follows: the requirements for the establishment of European Programme for Critical Infrastructure Protection; the concept's delineation; the actions needed to implement the concept; the definition of critical infrastructures at EU level; the definition of national critical infrastructures;the role of the state, owners and operators of critical infrastructures;the information flow iwithin the Critical Infrastructure Warning Information Network (CIWIN); providing financial support for EU member states to undertake activities in the filed under discussion; evaluation and monitoring of the activities/missions undertaken in the filed of critical infarstructures.

The European Programme for Critical Infrastructure Protection mission specifies that the EU cannot provide the protection of all critical infrastructures. Thus, even though the transnational character of vulnerabilites requires an integrated approach at the level of the Union, each member state needs to develop supplementary national programs and make areal contribution concerning national capabilities engagement to the benefit of the orther EU states.

The definition provided by the European Programme for Critical Infrastructure Protection for critical infrastructures identifies these as the networks, services, physical activities and information means that, if disrupted or stalled, can seriusly impact the health, safety, security and economic welfare of the citizens or state governance.

The goals of EPCIP are as follows: to identify and list, with the support of the member state governments, the critical infrastructures identifiable at national level in accordance with the priorities established by EPCIP; to ensure the collaboration of organizations and governments in information dissemination and risk reduction in order to counter any events that may lead to extended or long-lasting disruption of critical infrastructures; to ensure a common approach to critical infrastructures management through the collaboration among private and public stakeholders.

Another goal of EPCIP is to join in a network all national representatives and specialists in critical infrastructure protection from all EU member states. Thus, the proper functioning of the Critical Infrastructure Warning Information Network – CIWIN established in 2005 is ensured.

As far as the latter is concerned, its goal is to encourage information exchange about the common threats and vulnerabilities, as well as to contribute to the adoption and implementation of the necessary measures and strategies aimed at limiting risk impact and at protecting the critical infrastructures.

2.3.4. The EPCIP critical infrastructures taxonomy

As a result of the numerous investigations and research undertaken in the filed, the EPCIP, launched in 2006, December 12 mentions a number of critical infrastructures identified within the EU. These cover 11 critical sectors and 32 servces related to these4, as presented in **Table no. 1.**

Table no.1 Critical infrastructures: critical sectors and related services

Sector	Product or service
I. Energetic	1. Oil and gas production, refineries, storage facilities, pipelines; 2. Electrical energy production; 3. Gas, oil, electrical energy transprotation; 4. Gas, oil, electricity distribution activities.
II. Information and communication technology	5. information systems and networks; 6. Command and automation systems; 7. Landline and mobile communication services; 8. Radiocommunication and bavigation systems; 9. Sattellite commmunication services; 10. Radio services;
III. Water supplies	11. Drinkable water supply; 12. Water quality control; 13. Dam building and water quantity control;
IV. Food supplies	14. Food supplies, food security and safety;
V. Health	15. Medical care; 16. Drugs and pharmaceuticals; 17. Biolaboratories şi bioagents;
VI. Financial	18. Payment services and related facilites; 19. Government financial systems;
VII. defense, public order and national security	20. National defense, public order and national security; 21. Border integrated management;
VIII. Administration	22. Governance; 23. Armed forces; 24. Services and administration; 25. Emergency services;
IX. Transportation	26. Roads;27. Railways; 28. Naval, river, maritime and ocean trasports; 29. Air transport;
X. Chemical and nuclear industry	30. Chemical and nuclear substances processingand storage; 31. Pipleines for hazardous chemical substances and products;
XI. Space	32. Air traffic.

3. CONCLUSIONS

The traditional concepts of physical protection and security have evolved as a result of the direcst, visible and immediate threats posed by a globalized world. Moreover, the concepts of risk, vulnerability or asymmetric threats have been resignified and coined. The numerous events that have occurred lately and their effects have heavily influenced the debtaes of the specialists and of the civil society representatives. Worth reminding in this respect of the following: the terrorist attacks on air, road, railway, underground transportation, on information systems, the natural distaers, the human mismanagement of critical systems, major technological accidents, cyber attacks, etc. Therefore, the intiatives in the field of critical infrastructure protection mentioned by this article express the concern on behalf of the governments and international organizations for the citizens' welfare.

REFERENCES

[1] Monitorul Oficial al Romaniei, part I, no. 757, 12 Nov. 2010*: Government Emergency Ordnance no. 98/2010 on the identification and protection of critical infrastructures. CIN is also defined by the EC* Directive 114/2008, of 08 December 2008.

[2] Decision no. 718 of 13 July 2011 concerning the approval of the National Strategy on critical infrasructure protection.

[3] dr. Alexandrescu, Grigore; dr.Văduva, Gheorghe, Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție, Carol I National Defense University Publishing House, Bucuresti, 2006, p. 8.[4] prof. univ dr Rizea, Marian; Marinică, Mariana; Barbăsură, Alexandru; drd. Dumitrache, Lucian; Ene, Cătălin, Protecția infrastructurilor critice în spațiul euroatlantic, Ani, 2008, Bucuresti, p.7.