CRITICAL INFRASTRUCTURE PROTECTION-THE FOUNDATION OF NATIONAL SECURITY (2)

Mihai-Marcel NEAG
mmneag@yahoo.com

"NICOLAE BĂLCESCU" LAND FORCES ACADEMY, SIBIU, ROMANIA

ABSTRACT

The development of the society and the insurance of a high level of the quality of life for citizens is a permanent concern, both at national and European level. The protection of the critical infrastructures is a precondition to ensure the continuity of economic activities and the creation of an appropriate framework for the development in a complex and uncertain security environment. The concept of critical infrastructure has gained great importance for both countries and for political, economic or military alliances, due to the interdependencies created between the various critical objectives and their vital importance to the security, economy and safety of the population. Being of utmost importance for each and every state, we should take a closer look to the problems of the critical infrastructures protection.

The legal framework in which the margin for critical infrastructure protection must be developed with more attention, taking into account the operation of the public-private partnership in the field of critical infrastructures, as well as the obligations arising from the quality of Romania as member state of the European Union and NATO.

Keywords
National and European critical infrastructures, national security, protection

1 Introduction

The trends and current geopolitical and geo-strategic perspectives expand, more and more, the concept of “national security” on the economic, information technology and communication, diplomatic, environmental components. Critical infrastructures are usually vulnerable to the actions of some external/internal factors and they are under the risk to be destroyed or made non-operational.

The development of the society and the insurance of a high level of the quality of life for citizens is a permanent concern both at national and European level. The protection of the critical infrastructure is a precondition to ensure the continuity of economic activities and the creation of an appropriate framework for the development in a complex and uncertain security environment. In the field of critical infrastructure, the energy, transport and telecommunications sectors are the most exposed to the risks and threats that may affect the state of national security. The interrelationship between these sectors, their operation integrated into complex systems infrastructures, requires a permanent assessment of the challenges posed by new risks and threats to promote rules, attitudes/behaviors, accepted and assumed by public opinion.
The recent developments on the world geopolitical scene that have targeted actions against national interest objectives with influence on the economic and social life, demonstrate us how vulnerable certain areas or sectors of activity can be, which provide essential services to all areas of social life. In this context, more attention should be given to these areas directly related to civil society, but also to the national security, given the scale and the effects of the negative consequences that can result from the disruption of the functioning of these areas or sectors of activity which are generically called “critical infrastructures”.

Critical infrastructures issues represent a topic of utmost topicality and the critical infrastructure protection is a relatively new field that requires an integrative, systemic and comprehensive approach to safety objectives. Protecting the vital components that make up the critical infrastructure helps avoid critical situations that may generate negative consequences with sudden changes in the socio-economic life.

Ongoing assessment of the condition of the infrastructure in general, those critical, in particular, allow the specification of their protection responsibilities, integration of forces and means of action in a particular flexible system, one of response to possible risks and threats. Reducing critical infrastructure vulnerabilities also involves a partnership between the various actors with common interests (business, governmental, academic environments as well as the civil society) in which the State should have a stimulating, coordinating role in the development of such networks. The vulnerabilities of critical infrastructures have been spoken of in recent years amid growing terrorist acts, deliberate interruption of the supply of energy materials at the level of States, of technological accidents due to human errors or of the effects of disasters/natural disasters.

Any inefficiently managed/protected infrastructure may be in critical situations, marked by moments of organizational/operational crisis, which may lead to sudden, decisive changes, with negative consequences in the national security plan, mostly because the “critical infrastructures” are complex systems of network type or contain such subsystems; specific targets of national importance can also be included.

The complexity of the protection of the critical infrastructure needs to be addressed from at least three perspectives: as a function of systems, operations and processes; as an associate security system created by other structures and as a function of meta-system or as system of systems. [1] The protection of critical infrastructures has generated both ways of identifying the degree of safety of the critical objectives and action procedures set out in the strategies developed by each State. When it comes to these strategies, we note the existence of a correlation with the systems in which these strategies are integrated (NATO, EU), in order to achieve a continuous and coherent partnership across all states, at European and world level.

2. The European Approach to Critical Infrastructures Protection

The entire Euro-Atlantic space has resized the policy and strategy with regard to securing critical infrastructures. The critical infrastructures issue is in the attention of the European authorities. The EU national security strategy is intended to enable Europe to respond to the challenges of existing and emerging threats, according to a common approach involving both the EU actors as well as those at national and local levels. The loss of or damage to critical infrastructures could have serious consequences for society. The action plan on the protection of critical infrastructures is built on five pillars: preparation and prevention, detection and response, mitigation and recovery after incidents, international cooperation and criteria for the European critical infrastructures in the different sectors.

The dramatic events of September 11, 2001 in the United States of America, as well as of March 11, 2004 in Madrid, as
well as those of July 2005 in London, confirmed that modern societies are becoming increasingly vulnerable to terrorist attacks and asymmetric threats, affecting, in particular, the safety of the individual and the security of essential infrastructures, which constitute the structure of resistance to any companies or networks vital for the functioning of the society as a whole [2].

The assessment of the impact accompanying the action plan on the protection of critical infrastructures, as well as a number of analyses and reports made by interested parties in the public and private sectors highlight the constant increase in the number, scale and impact of threats, whether it is natural threats or ones generated by people. The global geopolitical dimension of the new types of threats is becoming more and more obvious. We are currently witnessing a trend to use information and communication technologies for political, economic and military supremacy including through the offensive capabilities.

According to the overall strategy concerning the strengthening of the critical infrastructures and their protection, drawn up by the European Commission, the critical infrastructures include:

– installations and networks in the energy sector (in particular production plants of electricity, oil and gas storage facilities and refineries, transmission systems and distribution);
– technologies for communications and information (telecommunications, broadcasting systems, software, and networks, including the Internet, etc.);
– financial sector (banking, stock markets and investments);
– the health care sector (hospitals, care facilities and blood banks, laboratories and pharmaceuticals, emergency services, search and rescue);
– food (food security, means of production, distribution and food industry);
– water supplies (stocks, storage, treatment and distribution networks);
– transportation (airports, ports, intermodal facilities, railways, mass transit networks, traffic control systems);
– production, storage and transport of dangerous goods (chemical, biological, radiological and nuclear materials);
– administration (basic services, facilities, information networks, assets, important places, national monuments) [3].

The implementation of a European program for the protection of critical infrastructures (EPPCI) emerged as a necessity to establish unitarily in EU, the principles and tools needed to improve the protection of critical infrastructure in the states of the Union. This program has been extensively prepared during 2005.

The European Commission, at the request of the Council of Justice and Home Affairs, adopted this communication and a proposal for a directive regarding the identification and ranking of critical infrastructures, in order to improve their protection.

The legislative framework for EPPCI consists in the following [4]:

– a procedure for identifying and classifying the European critical infrastructures and a common approach to assess the need to improve their protection;
– measures designed to facilitate the implementation of PEPIC, including an action plan EPPCI, the network of alert concerning critical infrastructures (CIWIN), the setting up of some expert groups on the critical infrastructure protection (CIP) at European Union level, the processes of sharing information on PIC and identification and analysis of interdependencies;
– support for the member states of the European Union concerning national critical infrastructures (NCI) which can be used optionally for a given member state and emergency planning;
– an external dimension;
– financial support measures, in particular the specific EU “Prevention, preparedness and consequences of the management of terrorism risks and other
security-related risks”, to provide funding opportunities for measures related to the protection of critical infrastructures.

This action plan, structured in three main directions of work, is a continuous process and requires periodic assessment.

The development and application of EPPCI meant the completion of stages:
- In October 20, 2004, the Commission published a communication on Critical infrastructure protection in the fight against terrorism;
- the Commission’s intention to propose a European program for critical infrastructure protection (EPCIP) and a critical infrastructure warning (CIWIN) was accepted by the European Council of 16 and 17 December 2004, both in its conclusions on Prevention, preparedness and response to terrorist attacks, as well as in the Solidarity program adopted by the Council on 2 December;
- In September 15, 2005, a decision on the financing of a pilot project that included a set of preliminary actions designed to strengthen the fight against terrorism was adopted. This was followed by a second decision, on 26 October 2006 on the financing of the pilot project of EPCIP;
- In November 17, 2005 the Commission adopted a green paper on the European program for critical infrastructures protection;
- In December 12, 2006 the Commission presented a proposal for a directive on the identification and ranking of European critical infrastructures and a common approach to assess the need to improve their protection. On the same day the Commission adopted this communication too. These documents provide a clear picture of how the Commission proposes to address the issue of protection of critical infrastructures in the EU.
- In February 12, 2007, the proposal concerning the specific program Prevention, preparedness and consequences of the management of terrorism risks and other security-related risks was adopted;
- April 13, 2007, the European Central Bank has endorsed the draft directive of the Council of the European Union concerning the identification and ranking of European critical infrastructures and the assessment of the need to improve their protection.

As we can notice, the European Union's aim was to achieve a common policy in the field of critical infrastructures protection. The primary and final responsibility for the protection of the European critical infrastructures (ECI) lies with the member states and the owners/operators of such infrastructures. [5]

Even a non-military organization such as the EU struggles with the issue of

---

**Figure no. 1 – Main directions of work of EPPCI**

The development of measures horizontally applicable to all activities in the field of PIC

The protection of European critical infrastructure in order to reduce their vulnerability

Creating a national framework designed to help member states to protect their national critical infrastructures
whether there should be a focus on terrorist threat or if it needs a general approach. Another problem that stands in front of a less military organization and thereby less hierarchical is the assignment of authority: will it be a network of national contact points or will a single supervisory body at the European Union level be formed.

The European approach to critical infrastructures protection focuses mainly on the following procedure: ensuring the legal framework (which contains the rules governing the identification of critical infrastructures, risk assessment and the identification of priorities in terms of countermeasures and procedures); identification/designation of the critical infrastructure as a European critical infrastructures (ECI); issuing of the security plan in accordance with European and national norms in force in the Member States; the establishment of liaison officers for security for all European and national critical infrastructures.

3. NATO’s Role in Critical Infrastructures Protection

NATO was the first international organization that took concrete actions related to critical infrastructure protection. NATO’s interest in the protection of the critical infrastructures began in 2001 and has been progressively consolidated by several policy documents and programs.

It is important to keep in mind that the accents NATO has in view, will be different from those used in the EU or other international organizations, and of course, at the national level. NATO believes that PIC is primarily a national responsibility and wants to focus on the role of coordination between the Organizations of Nations, and the role of the authority responsible for its own infrastructures.

The body of the Alliance, which has the responsibility to find solutions to a uniform approach to the problems related to the criteria to determine the critical infrastructures, the methods of risk analysis and fixing vulnerabilities, as well as their methods of protection, is The Superior of Civil Emergency Planning (SCEP). It has an important role in coordinating the activities of the bureaus of Planning and committees; ensuring of the integrated character of the contributions, as well as the functional aspect of the work done; the study of the way in which Nations may be assisted, in the most efficient manner; ensuring coherence in policy development concerning additional measures to improve civil preparedness and vulnerability reduction of the Organization.

Therefore, the SCEPC will actively pursue information exchange in the framework of NATO's cooperation with all relevant bodies, as well as the UN and the EU, the latter is considered to be a priority in most NATO countries which are subject to the guidelines of the Organization master. The holistic perspective on the new threats of NATO's Strategic Concept represents an important first step in an attempt to make CIP a legitimate theme of the Alliance. A second step is to provide CIP a distinct organizational framework, within NATO’s International Secretariat. Alongside the internal analytical capacity expansion of NATO and a better exchange of information and intelligence among allies, the new security challenges – including those targeting CIP – are reflected now at the level of the organizational structure of NATO. The third step towards a more systematic approach of NATO regarding ICIP lies in achieving a sustained dialogue with other organizations such as the EU and the OSCE.

Having in view of the different opinions of the allies, it would be a success if it would be able to make PIC a topic for discussions, the same as those against cyber attacks and the prevention of the proliferation which are already common points on NATO’s political agenda. Such an institutionalized dialogue between the allies is an initial condition to determine the next steps, such as, for example, conducting of discussions among the North Atlantic Council and
different partner countries or groups of partner countries (the so-called formula '28+n') on the topic of CIP or setting up teams for the preparation and reform of the defense for the protection of critical infrastructures. At the military level, some of the NATO operations, such as Ocean Shield Operation to combat piracy, can contribute to securing shipping routes for fuels.

The activity of the protection of critical infrastructures may not take into account the national boundaries and involve joint efforts, for the purpose of identification and assessment of any of their vulnerabilities. Thus, the protection of critical infrastructures – the key for maintaining the stability and security – requires the amplification of the concerns of the main international actors (states and international organizations) for the development and harmonization of strategies in this field. They must allow for the identification and early warning of the risks, as well as the adoption and timely initiation of decisions/warnings of preventive interventions and countermeasures. [5]

The responsibility to identify, evaluate, and protect and secure the critical infrastructures, while the interdependencies grow, the vulnerabilities are obvious and the proliferation of threats to them emerge, it gets international values and valences, becoming a vital issue to the proper functioning of the society.

4. Conclusions

The new international requirements of the critical infrastructures and their protection, existing at both the European Union and NATO level is an imperative for the national authorities to develop and implement a uniform policy in this sensitive area of the contemporary world. International standards and legislation drawn up at EU level as well as on the part of NATO, is the basis for developing a strategic long-term vision for identification, risk analysis, vulnerability assessment and protection procedures for the national and European critical infrastructures on a national territory.

The critical infrastructures remain in an area which requires very well investigated, monitored, analyzed, evaluated, and improved forecasts. All States, the European Union, as a whole, United States of America and other countries, alliances, international security structures and regional authorities are intensifying their efforts to identify, monitor, optimize and protect the vital infrastructures of the countries, companies, and networks of the world.

The European approach to the protection opens the borders towards the new “protection zones” in particular, the motivation being due to the actions of the terrorist entities, after the bombings in Madrid (2004) and London (2005).

The concept of critical infrastructures has gained great importance for both countries and for political, economic or military alliances, due to the interdependencies created between the various critical objectives and their vital importance to the security, economy and safety of the population.

The international consequences in the field of critical infrastructures and their protection, existing in the EU and NATO, represent for all states the basic elements in developing their own strategies and the development of a risk management and improvement of the ability to respond to threats.

The critical infrastructures protection is connected to the need to maintain the viability of society starting with the administration, the economic, financial institutions, those of social welfare and health, the intelligence community, the military and civil protection and ending with supplies of food, water and energy, transport, communications, education, etc.

The new international requirements of the critical infrastructures and their protection, existing at both the European Union and NATO level is an imperative for the national authorities to develop and implement a uniform policy in this sensitive area of the contemporary world.
International standards and legislation developed at European Union level, as well as on behalf of NATO, are the basic elements for the drafting, at national and sectoral level, of a long-term strategic vision for the identification, risk analysis, vulnerability assessment and procedures for the protection of national and European critical infrastructures on a national territory, as well as a good risk management and an improvement in the ability to respond to threats.

References

5. If necessary, the Commission may set up expert groups in the field of CIP at EU level, in order to examine specific issues. According to the critical infrastructure sector, the experts’ functions may include: assistance in identifying vulnerabilities, interdependencies and best practice in the sector; developing measures to reduce vulnerabilities and devising performance indicators; formulation of case studies.