Annals of the Academy of Romanian Scientists
Series on Engineering Sciences
ISSN 2066-8570 Volume **2**, Number **1**/**2011**

CRITICAL INFRASTRUCTURES PROTECTION A ROMANIAN PERSPECTIVE (PART 1)

Liviu MURESAN[1], Septimiu CACEU[2]

Rezumat. *În fiecare stat membru al Comunității Europene există un număr de infrastructuri critice a căror perturbare sau distrugere ar influența semnificativ menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, ar avea un impact semnificativ la nivel local, regional și național, ca urmare a incapacității statului de a menține respectivele funcții, având totodată și efecte transfrontaliere similare. Acestea ar putea include efecte transfrontaliere intersectoriale ce rezultă din relațiile de interdependență dintre infrastructurile interconectate. Programul European privind Protecția Infrastructurilor Critice (EPCIP) lansat la 12 Decembrie 2006, definește sectoarele și serviciile critice aferente, promovând protecția acestora printr-o abordare care să acopere toate riscurile. Directiva CE 114/2008, care constituie un prim pas în cadrul unei abordări pas cu pas în direcția identificării și a desemnării ICE și a evaluării necesității de îmbunătățire a protecției acestora, se concentrează asupra sectorului energetic și a sectorului transporturilor, stabilind procedura pentru identificarea și desemnarea infrastructurilor critice europene ("ICE"). Romania, ca stat membru al EU este obligată să ia măsurile necesare pentru a se conforma Directivei CE 114/2008, până la 12 ianuarie 2011, dată când va informa Comisia cu referire la armonizarea legislativă, măsurile stabilite, precum și tabelele de concordanță menționate în această directivă europeană.*

Abstract. *In each EU Member States there are a certain number of critical infrastructures, the disruption or destruction of 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 at community, regional or Member State level as a result of the failure to maintain those functions and at the same time with significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. The European Program for Critical Infrastructure Protection (EPCIP) launched on 12 December 2006 has defined a list of European critical infrastructures and promoted their protection taking in consideration all hazard approach concept. The Directive EC 2008/114 constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection, concentrate on energy and transport sectors, establishing the procedure for the identification and designation of European critical infrastructures ("ECIs"). Romania, as EU Member State, shall take the necessary measures to comply with this Directive by 12 January 2011, date when shall inform the Commission with legislative harmonization aspects and communicate the text of those measures and their correlation with this Directive.*

Keywords: critical infrastructures, protection, concept, energy, directive, European program

[1]Ph.D., Executive President, EURISC Foundation, Romania, muresan@eurisc.org.
[2]Ph.D., Eng., Project Director, Research Coordinator, EURISC Foundation, Romania, septimiu@eurisc.org.

1. The Critical Infrastructure Concept

Infrastructures are essential for economic prosperity, national security and the quality of life in any country. Securing the functioning of this infrastructure is thus a measure by which the society aims to secure its present and develop its future.

Infrastructures can be grouped into three large categories, depending on their location, role and importance for the stability and functioning of the society, as well as for the safety and security of systems:

- ordinary infrastructures;
- special infrastructures;
- critical infrastructures.

Ordinary infrastructures represent a structure, a frame, which enables the developing and functioning of the system. These infrastructures do not present special qualities beside those which justify their existence and presence within the frame of systems and processes.

A country, for example, will always have roads, railways, towns, schools, libraries etc. As time goes by, some of these may become special, or even critical, depending on the new role they may have, on the dynamic of their importance and other criteria. For example, towns which have airports, powerful communication centres, nuclear plants, rail way knots etc. can be part of special infrastructures and, under circumstances, even part of the critical ones.

The special infrastructures play a particular role in the functioning of systems and processes, ensuring those with enhanced efficiency, quality, comfort, performance. Generally, the special infrastructures are performance infrastructures. Some of those, especially the ones which through extension or transformation (modernisation) can have an important role in the stability and security of systems, can also be critical infrastructures.

Critical infrastructures are generally those on which depend the stability, safety and security of systems and processes. They can be part of the special infrastructure category. However, it is not mandatory that all infrastructures which are or can become at some point critical, be part of the category of special infrastructures.

Depending on the situation, other elements can also intervene and even some of the ordinary infrastructures – as for example country roads, irrigation systems etc. – become critical infrastructures. This leads to the conclusion that there is a flexibility criterion in the identification and evaluation of such structures.

The European Programme for Critical Infrastructure Protection proposed in 2006 this definition: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed,

would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the member states.

Infrastructures are accounted to be critical due to:

- Singularity within the frame of infrastructures of a system or process;
- Vital importance as a material or virtual (net-like) support in the functioning of systems and the unfolding of processes (economic, social, political, military, informational, etc.);
- Important, non-replaceable role, which they play in the stability, reliability, safety, functionality and, especially in the security of systems;
- Increased vulnerability to direct threats, as well as to threats targeting the systems these infrastructures are part of;
- Special sensitivity in case of variation of the conditions and, especially in case of sudden changes of the situation.

The importance of critical infrastructures result also from the fact that they can be defined as being those industrial capabilities, services and facilities which, in case of interruption of their normal functioning, can affect human life, and, moreover, can harm or destroy human life. The protection of life and of the lifestyle of people envisages especially the preservation of the continuous functioning of these services and facilities.

The on-going increase of the complexity of processes and systems has led, inevitably, to the increase in the interdependence among the various categories of critical infrastructures. The existing global infrastructures are thus more and more dependent on high technology systems for the distribution of information, such as the Internet, without having a central administrative control and without a common security policy relative to the spreading of new types of threats.

In the same time, these infrastructures are more and more interdependent and dependent on each other in order to function properly. So, malfunction of one element can lead to disturbances in other critical infrastructures elements (cascade effect).

These modern infrastructures are based on the ability of interconnecting systems and networks and of offering global coverage for the transmission of information. The protection of systems and networks for the transmission of information requires new concepts and instruments for the behaviour analysis of these systems and of their impact on the infrastructures they are serving.

Identifying, optimizing and securing critical infrastructure is an undisputed concern, both for the managers of systems and processes, as well as for those aiming to attack, destabilize or destroy the systems and processes envisaged.

Critical infrastructures are not and do not become critical only because of attacks, but also due to other causes, human, as well as technical, some of them difficult to be identified and analysed. Generally speaking, especially after the terrorist attacks of the 11th September 2001 on the World Trade Centre and Pentagon, it is considered that infrastructures are or can become critical due to terrorist attacks or other threats, especially asymmetrical ones.

This is only one aspect or criterion for the identification of critical infrastructures. However, there are also other criteria, which depend both on the stability and functioning of systems and processes, as well as on the interconnectivity of those with the exterior environment. In this context, the analysis of the critical infrastructures issues has to take into account all dimensions and implications of the systems' and processes' stability and functionality, as well as the causal interlinking that can generates or influence their dynamic.

The criteria used for such analysis is variable, even if their area of coverage could be the same. The predominant criteria for analysis, mentioned in the specialized literature are the following:

- Physical criterion, regarding the positioning within other infrastructures (size, spread, endurance, reliability etc.);
- Functional criterion, regarding the infrastructure's role (what exactly does it "do");
- Security criterion (what is its role for the overall safety and security of the system);
- Flexibility criterion (reflecting the dynamic and flexibility in defining infrastructures as critical; some of the ordinary infrastructures become under certain circumstances critical ones and vice-versa);
- Unpredictability criterion, (considering that some of the ordinary infrastructures can become suddenly critical infrastructures).

Critical infrastructures have at least three components of critical phases:

- Internal component, defined through the increase (either direct or induced) of infrastructure vulnerabilities with an important role in the functioning and security of the system;
- External component, referring to the exterior stability and functioning in relationship to the systems the infrastructure is integrated in or associated to;
- Interface component, defined through the multitude of neighbouring infrastructures, which do not belong to the system as such, but influence its stability, functioning and security.

2. The geopolitics of critical infrastructures

Besides to the classic civil protection concept, to forms of "physical protection" of citizens, and protection against imminent threats, new vulnerabilities have evolved in the modern, increasingly globalized societies.

Terrorist attacks on air, rail, underground, road means of transport or on key information systems have had an impact on government-level debates and on political and military decision-making, as well as on the documents and decisions issued after 11 September 2001.

Critical infrastructure protection can be approached from three angles:

a) Many of the currently operational critical infrastructure systems are the consequence of the Cold War both in the west and in the east (especially the communist system inheritance).

b) The prospect of new types of vulnerabilities, the preservation of key critical infrastructures operational, and the need for modernization require considerable financial support. Critical infrastructures in the spatial dimension had not suffered major events until the Tamil Tigers attacked a satellite. A three-week waves of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, was causing alarm across the European Union and NATO alliance, both structures examining the offensive, its implications and further required measures. Since the beginning of 2008, the submarine dimension has suffered several optical fibre cable cut-offs, thus affecting the Internet information transfer across the continents, with damages that has not been well quantified yet. The attacks on those cables highlighted the enormous amount of Internet traffic that uses the undersea cable system, which carries many times more traffic than the satellite system does

c) The possible start of a new Cold War, involving issues of energy security and information security, will have effects that can hardly be estimated at present. Both the United States and Russia have therefore taken due action, but the "play" has grown more complex due to the experience and importance of new actors coming from Asia region.

Following these new dimensions of risk and vulnerabilities we can speak about critical infrastructure geopolitics mainly in the sector of energy security, but new sectors, from critical infrastructures of water supply and food supply security could be added in the following years..

Given the circumstances, new developments may occur, each calling for a complex assessment of certain systems, or systems of systems, as well as for specific measures.

Firstly, there is a need for developing the ability to forecast and interpret specific events that are going to take place or have already started. Natural hazards, man-made disasters, technical accidents, the intervention of an external criminal hand, of an "internal enemy", or a possible terrorist attack are rather hard to identify and determine in the early stage of a major event.

Secondly, increasingly complex systems, the interdependence existing among various categories of critical infrastructures call for expert interdisciplinary training that includes both international experience and concrete aspects deriving from "lessons learned" from previous events.

Within this context, the top management of public and private enterprises must provide more time and resources (financial, human, and material) to the people responsible for the smooth functioning of the critical infrastructures existing on their premises, as well as of those connected to national and transnational networks.

At the same time, specific *"security culture"* action is needed to ensure a flow of correct, complete, and timely information not only for own employees, but also for the public opinion, and especially for the local communities where the institutions operate.

Thirdly, given the security environment dynamics, it is necessary to be aware of the new threats to date, and of the respective vulnerabilities for critical infrastructures. New vulnerabilities can thus appear for any critical infrastructure, but also for the "nodal points" where they are interconnected with local, national, and international networks.

Fourthly, based on objective prioritization, authorities should build a list of critical infrastructures, which require protection measures. Due to objective reasons, limited budgets, lack of qualified personnel, lack of specific protection technology, and lack of time to find solutions in complex situations, authorities cannot take extensive measures for the protection of all of critical infrastructures at the same level.

A choice among ordinary infrastructures and specific infrastructures can be made starting from the "history of events" reported at national level, international experience, specific classified information and alerts received from special services, et al.

In the fifth place, the decision of taking protection measures in a specific case is accounted for not only by technological considerations, but also by political, social, economic, and cultural implications. Smooth functioning or, conversely, malfunction in some critical infrastructures that directly affect the quality of life and the functioning of modern society (electricity, water supply, heating, transportation, health care, waste disposal, et al.), having a direct impact on

citizens, can bear a high political cost. Therefore, political decision-makers will carefully monitor the reactions if such situations occur, particularly of those "charged with electoral potential".

In the sixth place, the authorities and the leadership of both the public and private sector fail to employ staff and provide all the resources in time, when it comes to highly specialized critical infrastructures such as the ones in the information systems sector. The training and the stability of highly qualified information specialists are challenges of all sectors with workforce mobility in a competition environment.

In this sector, specialists are "headhunted" by institutions in the national security sector, by the IT sector, by finance and banking institutions, by the national and multinational private sector or by international organisations.

The outsourcing of IT services to overseas companies can provide well-paid jobs with delocalization at distances of hundreds or thousands of kilometres.

In the seventh place, the central and local authorities must be aware of the need for the continuous assessment of the state of infrastructures, particularly of critical ones, and to set specific standards and clear responsibilities for their protection. Suitable legislation is needed to set responsibilities for the authorities, key institutions, to integrate their activities into a comprehensive civil protection concept, to train the personnel having special responsibilities, to integrate all into a coherent, flexible system, et al.

In the eighth place, the public-private partnership is mandatory for critical infrastructures, considering that the majority percentage is owned by the private sector in this domain.

Legislation must provide acknowledgement and regulations with respect to mutual rights and responsibilities. There is a need for a continuous dialogue on critical infrastructure issues between the authorities and the private sector. The dialogue must start during periods of normal conditions so that cooperation could function smoothly right from the beginning of an emergency or critical situation.

In this respect, authorities must identify incentives for a functional partnership, and at the same times apply sanctions when the usage of specific infrastructures is obstructed.

A special case is that of foreign companies or institutions operating on the national territory, either independent firms or multinationals.

In the ninth place, the responsibility for providing information regarding the location, physical state, and legal nature of key critical infrastructures rest with the national and local authorities. Even though critical infrastructure protection

necessarily requires restrictive information circulation, the national database must be designed and managed according to the national legislation, as well as the regulations and obligations that are incumbent on Romania as an EU and NATO member.

Lastly, but at the same time first, critical infrastructures and the need for their protection are key issues that must be included in strategies of national security, energy security, information security, food supply security, health security, transportation security, et al.

A coherent national strategy of critical infrastructures, integrated into the network of the above-mentioned strategies, *is a determining factor for a nation's resilience capability.*

Recent international security evolutions have shown a period of relatively high instability, probably followed by a period of instability "stabilization".

In this context, we consider that several issues such as critical infrastructures, their protection and resilience could contribute to security and stability. If we compare a critical infrastructure system with an articulate concrete block (used for river bank stabilization), several articulate concrete blocks can be seen as a system of systems that could break the current "instability waves".

Given the latest critical sectors evolutions and the increasing level of globalization, we could consider a new concept of successful critical infrastructure governance, with good prospects of national, European and international implementation.

3. Critical Infrastructure Protection – the Approach at European and Euro-Atlantic Level

As natural disasters increase in amplitude and frequency, and as the terrorist phenomenon has an unprecedented scope, critical infrastructures require enhanced protection from threats and risks.

Because of that, governments worldwide show special concern for ensuring the security of the population and of the state authority.

In this sense, a first phase of the approach was to evaluate the vulnerabilities and the impact on society in case of infrastructure and services dysfunction.

In the last years, numerous states took robust actions in view of establishing a common language and way of action for the protection of objectives considered to be critical infrastructures.

The European states have generally included in the critical objectives category: telecommunications, water and energy sources, the distribution networks, the

production and distribution of food, the health institutions, the transport systems, the financial and banking systems, the defence and public order institutions (army, gendarmerie and police).

In this sense, a critical infrastructure represents a material good or a complex objective which is vital for the overall functioning of the economy and society and is usually interconnected to other infrastructures.

The protection of a critical infrastructure results from the complex of measures taken for the prevention and mitigation of the risks related to the stopping or destruction of an infrastructure – which would through the interruption of its functioning affect other economic processes, would make victims or would have a major impact on the good governance and the morale of the population.

National and international security depends to a very large extent on the critical infrastructures of society. But those are more and more vulnerable in the face of the more and more sophisticated means used for attacking them. The specialized literature encompasses a wide range of topics related to the protection of critical infrastructures.

In the analysis of this topic, two axioms are accepted:

- it is practically impossible to ensure 100% protection of a critical infrastructure;
- there are no unique or universal solutions for solving this problem.

There are several different ways suggested for approaching the protection of critical infrastructures:

- the protection of critical informational infrastructures, which takes into account only the security of IT connections and of the protection solutions thereof, the physical protection competencies of the other infrastructures being dissipated among different state and private organisations;
- All stakeholders should promote measures in order to ensure the uninterrupted functioning of the IT nets and of the physical elements of critical infrastructures. In many European states, the physical protection represents a component of the national civil protection system.
- Closer cooperation between the public and private sectors should be promoted to ensure the highest possible protection of the critical infrastructures, taking in consideration a new model of approach, generically called “all hazards approach” (taking all risks into account);
- All parts involved should establish a minimum mandatory system for the protection of the governing system and certain, vital state organisms. Analysts are

lately paying enhanced attention to organized cybernetic attacks, capable of destabilizing the national infrastructure, the economy or even all components of the national security. The technical complexity required for such an attack is rather high and partly explains why no such attacks have been recorded so far. There were cases where attackers exploited some vulnerability and demonstrated that they have even bigger destructive capabilities.

In peace time, interested persons or organisations can initiate sabotage actions on the state institutions, scientific research centres, private companies and other strategic objectives. In a scenario of confrontations, there is the possibility of preparing the ground for attacking within the cyber space, through mapping the information systems of the state, identifying the main targets and placing hidden entry points or other means of access within the national infrastructure.

During times of crises or war, adversaries can try to intimidate or block national political leaders' freedom of action, by attacking the critical infrastructures and the basic functions of the economy or by eroding public trust in the governing or informational systems. Cyber-attacks on the information networks of any country can have serious consequences, such as the interruption of the functioning of key components, causing losses of material and intellectual property or even of human lives.

4. European Critical Infrastructures

The actions mentioned earlier lead to the fact that a process was started at European Commission level, for the developing of normative proposals in the field of Critical Infrastructure Protection. These projects were finalised and presented to the European Parliament, some of them started in 2005 and the rest of the documents in December 2006.

The documents are currently being debated and the European Parliament will endorse the legislation, norms and recommendations, which shall define the critical infrastructures of European interest and regulate the measures for their protection in the context in which each Member state will be required to define and develop specific internal measures, taking especially into consideration the structures defined as vital at European level.

Up to the present moment, several counties - Austria, France, Germany, Great Britain, Italy, Norway, Sweden, Switzerland, and Spain have created specific organisms, have developed methodologies, and have allocated substantial funds for the protection of the infrastructures they defined as critical.

The European Council, at its June 2004 meeting, has required the European Commission and the High Representative to develop a global strategy regarding the consolidation of critical infrastructures and their protection.

Especially after the dramatic events of 11th September 2001 in the Unites States and 11th of March 2004 in Madrid, but also on 7th July 2005 in London, the risks associated to terrorist attacks on European infrastructures rose. The consequences of such attacks are considered to be variable.

It is being estimated that a cyber-attack would make few or no human victims as direct consequence, but could lead to the interruption of the functioning of the vital infrastructures. For example, a cyber-attack against the transmission networks would lead to the interruption of telephonic conversations, data transmissions, television and radio. Until the damage will be recovered, serious consequences can occur as a result the chain-like propagation of unpredictable events due to the social impact caused especially through the psychological effect on the population and the major effects on the governing act on local and state level.

There is however also another perspective regarding the attacks on the critical infrastructures. An attack on the command-and-control systems of chemical installations or of the transport and distribution networks for electrical energy, gas and oil products could cause many victims and significant material damage. Even more, due to the interdependence of interconnected systems, the effects could multiply and unfold in a chain reaction.

An attack on the electricity networks could have very big effects, both in terms of the functioning of industrial installations, computer networks, banking sector, communication networks etc. but - where there are no own electric energy sources - also on the vital medical equipment used for the patients undergoing surgery or under monitored control.

Long lasting electricity interruptions in large areas in North America and Europe pointed once again that infrastructures in the field of energy are especially critical and vulnerable.

According to definition mentioned by "*The 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*", Critical Infrastructures are: *"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 same document, define *"European critical infrastructure"* or *"ECI"* as 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.

According to the documents of the European Commission, critical infrastructures include:

- Installations and networks in the energy sector (especially the installations for producing electricity, oil and gas, installations for storage and refineries, transport and distribution systems);
- Communication and information (telecommunications, radio transmission systems, programs, the information materials and networks, including the Internet etc.);
- Finance (the banking sector, the stock market and the investments);
- Health care sector (hospitals, care equipments for patients and blood banks, pharmaceutics laboratories and products, emergency services, searching and saving services);
- Food sector (security, production means, distribution and agro-alimentary industry);
- Water supply (reserves, storage, treatment and distribution systems);
- Transport (airports, ports, rail ways, mass transit networks, traffic control systems);
- Production, storage and transport of dangerous substances (chemical, biological, radiological and nuclear materials);
- Administration (basic services, installations, information networks, assets, important places, national monuments). Those infrastructures belong to the public or private sector. This is why, in the conception of the European Commission, the public authority has to take the responsibility for consolidating and protecting these infrastructures.

To this, modern communication networks are added, including the Internet, the computer networks and the radio navigation through satellite.

Due to interconnections and inter-conditioning, an attack on one critical infrastructure can have an effect, as *"domino effect"* on other critical infrastructures, amplifying, sometimes dramatically, the consequences.

This interdependence brings about a significant rising of the vulnerabilities of the entire system and of all critical infrastructures. Therefore, it is highly possible, that paradoxically, in parallel to the process of European integration, the number of critical infrastructures rises. This is yet another very important conclusion for the analysis of critical infrastructures, with all their vulnerabilities and the threats they are facing continuous proliferation.

However, the critical infrastructures know a certain dynamic, some can become critical, others, protected adequately, can exit this category.

The European Commission suggests three essential criteria for the identification of potentially critical infrastructures:

- *Extent or surface*. The deterioration of the critical infrastructure is evaluated depending on the geographical region which would suffer consequences; the international, national, regional/ territorial or local dimension;

- *The degree of seriousness*. The incidence or degradation can be null, minimal, moderate or high. The main criteria for the evaluation of the degree of seriousness: economic incidence, incidence on the public, incidence on the environment, dependence, political incidence;

- *Effect in time*. This criterion shows the moment in which the degrading of the infrastructure can have a major incidence or a serious effect – immediately, after 24-48 hours, in a week or within a longer period of time.

It is the duty of every state that it identifies through the governmental structures the critical infrastructures on its territory. However, the European states are not alone, isolated, but in extremely tightly knit, complex relationships. The absolute independence concept has disappeared a long time ago. Europe becomes more and more interdependent and responsible for everything which is going on, not only in international relations, but also on the territory of each state.

This is why the process of identifying, analysing, evaluating and securing (protecting) critical infrastructures cannot be fragmented, and, even less, isolated. If a single state does not comply with its obligations to identify, the critical infrastructures on its territory, and to take the necessary measures for the mitigation of their vulnerabilities, for countering the threats and ensuring the necessary protection and security standards, the effects will be felt, one way or another, by all the other states. In other words, the responsibility for identifying, evaluating, protecting and securing critical infrastructures becomes in the context of increased interdependency and the proliferation of threats, a vital aspect for the good functioning of human society. This is another important conclusion for the management of critical infrastructure security.

The international dimension of this responsibility resides in the following reality:

- Most of critical infrastructures, or those that can become critical, outreaches the geographical area of one state;

- The increase of the vulnerabilities of critical infrastructures of one state determines, one way or another, the raising of vulnerabilities of all infrastructures in the area and/or network;

- The network configuration and philosophy accentuate the interdependence, and equally raise the vulnerabilities of all-participating structures, but also the capacity and force of resistance to perturbations and threats.

Obviously, it is not possible to protect all critical infrastructures completely and always. However, the prerequisites need to be created for their efficient management: evaluation of the threats they face, the system and process vulnerabilities to risks and threats, the international cooperation and the establishment of a system for their efficient identification, monitoring, evaluation and securing.

In this context, the management of security is defined by the European Commission as a *"deliberate process which envisages the evaluation of risk and the implementation of the actions aimed at bringing the risk at a determined and acceptable level, at an acceptable cost".*

This requires:

- Identifying the risk associated to the system and process vulnerabilities of the critical infrastructures, the dangers and threats these face;
- Analysing and evaluating the risk;
- Controlling the dynamics of the risk;
- Maintaining it within set limits.

Due to the complexity of the earlier mentioned aspects, the Programme of the European Commission envisages only the transnational critical infrastructures, the protection of the national ones remaining the responsibility of the Member States of the EU within a common framework.

In this sense, there are already numerous directives and regulations, which impose means and procedures for the informing on accidents, establishing intervention plans in cooperation with the civil protection, the administration, the emergency services etc. There are for example action and reaction programmes in civil and military emergencies, such as nuclear, industrial, chemical, environmental, oil-related accidents, natural disasters, etc.

The European Commission keeps strict evidence thereof, informs and reports every year the situation regarding the evaluation of risks, the development of protection techniques - that is the horizontal harmonization, coordination and cooperation. This communication of the European Commission, which involves all the analyses and sectors measures, constitutes the basis of a **European Program for Critical Infrastructure Protection (EPCIP)** and aims to find solutions for their security.

The 'European Programme for Critical Infrastructure Protection' (EPCIP) refers to the doctrine or specific programs created as a result of the European Commission's directive EU COM(2006) 786 which designates European critical infrastructure that, in case of fault, incident or attack, could impact both the country where it is hosted and at least one other European Member State.

The objectives of the program are:

- Identifying, through the governments of the Member States, all the critical infrastructures of each state, and adding them to a central inventory, according to the priorities established through EPCIP;
- The collaboration of enterprises and companies in the respective sectors along with the governments for the dissemination of and reducing the risk of incidents susceptible of creating extended or durable disturbances to critical infrastructure;
- The common approach to the issue of critical infrastructure security, thanks to the collaboration of private and public actors.

The European Program has targeted, among others, the reunion of every structure specialized into protecting critical infrastructure of the Member States in a network. This could lead to the development of an early warning network of critical situations **Critical Infrastructure Warning Information Network – CIWIN**.

The network has been operational since 2005. The main function of this network is encouraging information exchange regarding threats and common vulnerabilities, accomplishing an exchange of measures and appropriate strategies which enable reduction of risks and protection of critical infrastructures.

R E F E R E N C E S

[1] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT: Prevention, preparedness and response in terrorist attacks, Brussels 20.10.2004, COM(2004) 698 final;

[2] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT on the Prevention of the Fight against Terrorist Financing, Brussels, 20.10.200, COM (700) final;

[3] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT: Preparedness and consequence management in the fight against terrorism, Brussels, 20.10.2004, COM(2004) 701 final;

[4] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT: Critical Infrastructure Protection in the fight against terrorism, Brussels, 20.10.2004, COM(2004) 702 final;

[5] GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (presented by the Commission), Brussels, 17.11.2005, COM(2005) 576 final;

[6] 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;

[7] COUNCIL OF THE EU - PROPOSAL for a COUNCIL DECISION on a Critical Infrastructure Warning Information Network (CIWIN), 07 January 2009;

[8] COUNCIL OF THE EU – PROPOSAL for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Community guidelines for the development of the trans-European transport network;

[9] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT on Critical Information Infrastructure Protection, COM(2009) 149 final, Brussels, 30.03.2009;

[10] REGULATION (EC) NO 460/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 10 March 2004 establishing the European Network and Information Security Agency;

[11] CRITICAL ELECTRICITY INFRASTRUCTURE: Current Experience in Europe, Prof. Dr. Eng. Adrian Gheorghe, Dr. Eng. Dan Vamanu, CNIP06 Special Issue of International Journal of Critical Infrastructure, 2006;

[12] RISK AND VULNERABILITY GAMES. THE ANTI-SATELLITE WEAPONRY (ASAT), Prof. Dr. Eng. Adrian Gheorghe, Dr. Eng. Dan Vamanu, Int. J. Critical Infrastructures, Vol. 3, Nos. 3/4, 2007;

[13] CRITICAL INFORMATION INFRASTRUCTURE PROTECTION – organizational and legal aspects, Myriam Dunn, Isabelle Wigert, Adrian Gheorghe, CNIP06 Special Issue of International Journal of Critical Infrastructure, 2006;

[14] LEARNING FROM THE PAST – Electric Power Blackouts and Near Misses in Europe, *Markus Schläpfer, Hans Glavitsch*, CNIP06 Special Issue of International Journal of Critical Infrastructure, 2006;

[15] NON-BINDING GUIDELINES for application of the 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, EU Commission, Joint Research Centre, Ispra, Italy, EUR 236665 EN- 2009;

[16] CRITICAL INFRASTRUCTURES AT RISK: A EUROPEAN PERSPECTIVE, Prof. Dr. Eng. Adrian Gheorghe, Old Dominion University, VA, US and Dr. Eng. Marcelo Masera, EC Joint Research Centre, Ispra, Italy.