CRITICAL INFRASTRUCTURES PROTECTION A ROMANIAN PERSPECTIVE

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 inluența semnificativ menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, ar avea un impact semnificativ la nivel local, regional şi național, ca urmare a incapacității statului de a menține respectivele funcții, având totodata şi efecte transfrontaliere similare. Acestea ar putea include efecte transfrontaliere intersectoriale ce rezultă din relațiile de interdependență dintre infrastructurile interconectate.*

Programul European privind Protectia Infrastructurilor Critice (EPCIP) lansat la 12 Decembrie 2006, defineste sectoarele şi 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 şi a desemnării ICE şi a evaluării necesității de îmbunătățire a protecției acestora, se concentrează asupra sectorului energetic şi a sectorului transporturilor, stabilind procedura pentru identificarea şi 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 cand va informa Comisia cu referire la armonizarea legislativă, măsurile stabilite, precum şi 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

[1] Eng., PhD, Executive President EURISC Foundation – Romania, *muresan@eurisc.org;*
[2] Eng. PhD, Project Director - Research Coordinator EURISC Foundation – Romania, *septimiu@eurisc.org*

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. 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, railway 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, informational, military 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 ongoing 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 analyzed. 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, a.o.

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, a.o.), 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, a.o.

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, a.o.

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 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, analyzing, 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;
- Analyzing 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.

5. European Program for Critical Infrastructure Protection (EPCIP)

On the 12th of December 2006, the European Commission launched a package of measures for improving the Protection of Critical Infrastructures in Europe, comprising the following documents:

- Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Brussels, 12.12.2006, COM (2006) 787 final - 2006/0276 (CNS) (presented by the Commission) {SEC (2006) 1648} {SEC (2006) 1654}.
- Communication from the Commission, on a European Programme for Critical Infrastructure Protection, Brussels, 12.12.2006, COM (2006) 786 final.
- A Communication on Protecting Europe's Critical Energy and Transport Infrastructure.

The Vice President of The European Commission, Franco Frattini, the Commissioner for Justice, Freedom and Security, stated:

"The security and economy of the European Union, as well as the welfare of our citizens depend on certain infrastructures and services which these offer. Discontinuity in their functioning can generate losses of lives, losses of goods and the loss of public confidence in EU organisms. The package of norms we are presenting today aims to assure the Community that any eventual dysfunction or unwanted intervention over the critical infrastructures will remain in an incipient form, situations with reduced frequency, controllable, geographically isolated and with minimal effect, locally as much as possible."

In accomplishing and implementing the European Program of Critical Infrastructure Protection, the starting point was the complex reality, knowing that it is impossible for the European Union to actually protect all critical infrastructures. Therefore, the program is focusing only on the protection of the transnational critical infrastructures, while the protection of national critical infrastructures remains the responsibility of the EU Member States, but, obviously, as part of a common framework.

The European Program for Critical Infrastructure (EPCIP) has the following main objectives:

- Identifying and designating The European Critical Infrastructure and the measures that are imposed to protect and improve them. The proposed directive sets the procedures for the identification and designation of the **European Critical Infrastructure (ECI)** and the accepted measures for improving the protection of these infrastructures;
- The promotion of specific measures that facilitate the implementation of The European Program for Critical Infrastructure EPCIP, including a Plan of Action for The Protection of European Critical Infrastructures and Warning Information Network – CIWIN, involving a group of experts at European Union level, a system for permanent information exchange of useful information, as well as identifying and analyzing the interdependence of critical systems;
- Support for the member states regarding The National Critical Infrastructures (NCI), which can optionally be used by other countries;
- Financial support for some of the agreed measures and particularly for the EU Program regarding "Prevention, Protection and Removal of Terrorist Action Effects and Other Security Risks", for 2007-2013, providing financial support for Protecting Critical Infrastructures which have the potential to be transferred and applied at EU level.

This European Program is supported by a series of EU documents, with the objective of protecting some critical Infrastructures in the context of the fight against terrorism, developed and adopted at European Union level, before 12th of December 2006, as follows:

- 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;
- 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;

- 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;
- 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;
- GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (presented by the Commission), Brussels, 17.11.2005, COM(2005) 576 final;
- GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (presented by the Commission), Brussels, 17.11.2005, COM(2005) 576 final, is the framework document which defines the options on EU level, which, put into action, would ensure the improvement of prevention actions, preparation of the forces and specific response means and measures for the protection of EU's critical infrastructures.

The option presented in the EPCIP "Green Paper" are a combination of measures which must be accepted as complementary to the effort made by each nation in this field.

Identifying the national critical structures, adding them to a central inventory, the database and custom protection measures and interventions for every one of them, become confidential, but are not presented to the Commission, and the exchange of information will be made only between national authorities and the designated structure at the European Commission level with the management of the Critical European Infrastructure Protection.

The European Program for Critical Infrastructure Protection has in its attention 33 vital sectors and services connected to them.

Sector	Service or Product
I. Energy	1. Production of oil and gas, refinery, treatment and deposit, including pipelines; 2. Production of electric energy; 3. Energy, gas and oil transport; 4. Energy, gas and oil distribution;
II. Information and technology, Communication	5. Information and network systems; 6. Command, automation and instrumentation systems; 7. Mobile and land telecommunication services; 8. Navigation and radio communication services; 9. Satellite communication services; 10. Broadcasting services;
III. Water Supply	11. Drinking water supply; 12. Water quality control; 13. Dam building and water quantity control;
IV. Food Supply	14. Food supply, food safety, security and protection;
V. Health	15. Medical support and hospital services; 16. Drugs, serums, vaccines, and pharmaceutical products; 17. Bio laboratories and bio agents;
VI. Finance	18. Payment services / related structures; 19. Governmental financial systems;
VII. Defence, Public Order, National Security	20. Country defence, public order and national security; 21. Integrated management of borders;
VIII. Administration	22. Government; 23. Armed forces; 24. Administration and services; 25. Emergency services;
IX. Transport	26. Road Transport; 27. Railways; 28. Sea, river and ocean transport; 29. Air transport;
X. Chemical and Nuclear Energy	30. Production, processing and storing of chemical and nuclear substances; 31. Dangerous chemical substances pipes;

XI. Space	32. Air traffic 33. Outer Space (*Proposal made at ESRIF Workshop – September 2007 by Prof.Dr.Eng. Adrian Gheorghe, Dr. Liviu Muresan and Dr.Eng.astronaut Dumitru Prunariu – EURISC Foundation)*

Because a great deal of the elements that define critical infrastructures are private property, the security and control measures require the responsible involvement of both the private and public sector in form of public-private partnerships in implementing national interests.

The European Commission document presented to the European Parliament regarding "The Prevention and Response to terrorist threats" COM (2004) 698 Final, of 20.10.2004, clearly states the framework for "Public - Private Security Dialogue" as well as the role of the private sector alongside the public sector, in establishing and accomplishing the measures of risk reduction and intervention, channelled towards protecting critical sites in administration as well as assuring the security of goods and services vital to each country.

The national authorities, ministries, which manage critical infrastructures, most of the times, will have the competence of coordinating planned measures. Also, the aspect of trans-border interdependence protection measures has to be kept in mind, which explains the necessity that the EU would act or assume a role in coordinating certain situations.

The European Program of Critical Infrastructure Protection EPCIP has established that a communication from the European Commission is released, through which it states the stage of accomplishments and the necessary measures for the next stage. This document integrates different analyses and measures within different sectors of Member State economies. The Member State governments will continue to develop and update the database regarding the relevant elements of critical national infrastructure and will be responsible for its development, and also the validation and inquiry of important plans of action, assigned to assure the continuity of vital services in the event of an attack or the destruction of important sites and objectives found in their jurisdiction.

Also, the European Union constituted a committee of specialists with the authority to verify the norms and way of action of the Member States regarding the fight against cybernetic threats and attacks over critical infrastructure. As part of "The European Program of Coordinating the Research in the Domain of Critical Infrastructures", the CI2RCO project, launched in 2005 has the objective to identify and support research groups and programmes focusing on Informational Security Systems of Critical Infrastructure (IT Security), like telecommunication networks and electricity distribution networks. The purpose of

these cooperation programs is to reach out beyond the limits of the EU and include the USA, Canada, Australia and Russia as a research force.

6. Energy for Europe with a secure supply

At 19 September 2007 in Brussels a new momentum has been given to the energy policy for Europe. The European Commission has adopted a third package of legislative proposals to ensure a real and effective choice of supplier and benefits to every single EU citizen. The Commission's proposals put consumer choice, fairer prices, cleaner energy and security of supply at the centre of its approach.

The legislative package consists of:

- A Regulation establishing the EU Agency for the cooperation of National Energy Regulators;
- An Electricity Directive amending and completing the existing Electricity Directive 2003/54;
- A Gas Directive amending and completing the existing Gas Directive 2003/55;
- An Electricity Regulation amending and completing the existing Electricity Regulation 1228/03;
- A Gas Regulation amending and completing the existing Gas Regulation 1775/05.

The above mentioned package promotes sustainability by stimulating energy efficiency and guaranteeing that even smaller companies, for instance those that invest in renewable energy, have access to the energy market. A competitive market will also ensure greater security of supply, by improving the conditions for investments in power plants and transmission networks, and thus help avoid interruptions in power or gas supplies. Guarantees of fair competition with third country companies are also strengthened.

To make the internal market work for all consumers whether large or small, and to help the EU achieve more secure, competitive and sustainable energy, the Commission is proposing a number of measures to complement the existing rules.

Separation of production and supply from transmission networks: Network ownership and operation should be "unbundled". This refers to the separation between the network operation of electricity and gas from supply and generation

activities. The proposals make it clear that the Commission's preferred option in this respect is ownership unbundling - in other words that a single company can no longer own both transmission and be occupied in energy production or supply activities. In addition, the Commission proposes a second option, the "independent system operator" which makes it possible for existing vertically integrated companies to retain network ownership, but provided that the assets are actually operated by a company or body completely independent from it. Either one of these options will create new incentives for companies to invest in new infrastructure, inter-connection capacity and new generation capacity, thereby avoiding black-outs and unnecessary price surges.

The Commission recognizes the strategic importance of Energy Policy. Therefore the package contains safeguards to ensure that in the event that companies from third countries wish to acquire a significant interest or even control over an EU network, they will have to demonstrably and unequivocally comply with the same unbundling requirements as EU companies. The Commission can intervene where a purchaser cannot demonstrate both its direct and indirect independence from supply and generation activities.

Facilitating cross-border energy trade: The Commission proposes to establish an Agency for the cooperation of National Energy Regulators, with binding decision powers, to complement National Regulators. This will ensure the proper handling of cross-border cases and enable the EU to develop a real European network working as one single grid, promoting diversity and security of supply.

More effective national regulators: the Commission proposes measures to strengthen and guarantee the independence of national regulators in Member States.

Promoting cross border collaboration and investment: The Commission proposes a new European Network for Transmission System Operators. EU grid operators would cooperate and develop common commercial and technical codes and security standards, as well as plan and coordinate the investments needed at EU level. This would also ease cross border trade and create a more level playing field for operators.

Greater transparency: Steps to improve market transparency on network operation and supply will guarantee equal access to information, make pricing more transparent, increase trust in the market and help avoid market manipulation.

Increased solidarity: by bringing national markets closer together, the Commission foresees more potential for Member States to assist one another in the face of energy supply threats.

Customers will also benefit from a *new Energy Customers' Charter to be launched in 2008*. This will include measures to address fuel poverty, information for customers to choose a supplier and supply options, actions to lower red tape when changing energy suppliers and to protect citizens from unfair selling practices. A separate information campaign will inform customers of their rights.

The proposed package of measures was anticipated in the Commission's Energy Policy for Europe Brussels {COM (2007) 1 final / 10 January 2007}, which was endorsed by the European Council in March 2007. This set out the need for the EU to draw up a new energy path towards a more secure, sustainable and low-carbon economy, for the benefit of all citizens. Fully competitive markets are an essential pre-requisite to reaching this goal. From 1 July 2007, citizens across the EU already have a right to choose their supplier. The new package aims to ensure that all suppliers fulfil high standards of service, sustainability and security.

The Commission's proposals for the internal energy market are an integral part of the Lisbon Strategy and the EU's energy strategy and will be discussed among Heads of State and Government at their regular Summits.

7. 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.

On the 23rd of December 2008, the European Union published on the "Official Journal" the new "***Directive on the Identification and Designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection***" - COUNCIL DIRECTIVE 2008/114/EC.

This Directive establishes a procedure for the identification and designation of European critical infrastructures ("ECIs"), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of citizens.

The Council Directive 2008/114/EC, constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ("ICT") sector.

Member States must go through a process of identifying potential ECIs, with the help of the Commission if required. Member States should make use of a series of criteria to identify these potential ECIs. The cross-cutting criteria take

into account possible casualties and economic and public effects, while the sectors criteria consider the specificities of each ECI sector. This directive currently concerns only the energy and transport sectors and their subsectors as identified in Annex I. Additional sectors might be added with the review of the directive.

In the Annex I, are mentioned ECI sectors and sub-sectors, as follow:

I. Energy:

1. Electricity: Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity;
2. Oil : Oil production, refining, treatment, storage and transmission by pipelines;
3. Gas: Gas production, refining, treatment, storage and transmission by pipelines LNG terminals.

II. Transport:

4. Road transport;
5. Rail transport;
6. Air transport;
7. Inland waterways transport;
8. Ocean and short-sea shipping and ports

In terms of the energy sector and in particular the methods of electricity generation and transmission (in respect of supply of electricity), it is understood that where is deemed appropriate, electricity generation may include electricity transmission parts of nuclear power plants, but exclude the specifically nuclear elements covered by relevant nuclear legislation including treaties and Community law.

This Directive complements existing sectors measures at Community level and in the Member States. Where Community mechanisms are already in place, they should continue to be used and will contribute to the overall implementation of this Directive. Duplication of, or contradiction between, different acts or provisions should be avoided.

Each Member State should go through a cooperative designation process for potential ECIs located on its territory. This process involves discussions with other Member States, which could be significantly affected in case of the loss of service provided by an infrastructure. In order for an infrastructure to be formally

designated as an ECI, the Member State on whose territory it is located must give its assent.

The identification and designation of ECIs by Member States ***must be completed before 12 January 2011, after which they are to be reviewed regularly.***

The Member State on whose territory an ECI is located must inform the Commission annually of the number of potential and designated ECIs for each sector.

Member States must ensure that an **operator security plan (OSP)** or an equivalent measure is in place for each designated ECI. The purpose of the OSP process is to identify the critical assets of the ECI as well as the existing security solutions for protecting them. The minimum content to be covered is defined in Annex II of the directive. The OSPs must be reviewed regularly.

Member States must also ensure that a **security liaison officer or equivalent** is designated for each ECI. The officer serves as the contact point between the owner/operator of the ECI and the Member State authority concerned. The purpose is to allow for the ***exchange of information regarding the risks and threats relating to the ECI***.

Article 3 from Directive, requires each Member State to identify the critical infrastructures which may be designated as an ECI. This procedure shall be implemented by each Member State through the following series of consecutive steps:

Step 1. Each Member State shall apply the specific criteria in order to make a first selection of critical infrastructures within a sector.

Step 2. Each Member State shall apply the definition of critical infrastructure pursuant to Article 2(a) to the potential ECI identified under "Step 1".

The significance of the impact will be determined either by using national methods for identifying critical infrastructures or with reference to the cross-cutting criteria, at an appropriate national level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 3. Each Member State shall apply the transboundary element of the definition of ECI pursuant to Article 2(b) to the potential ECI that has passed the first two steps of this procedure. A potential ECI which does satisfy the definition will follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 4. Each Member State shall apply the cross-cutting criteria to the remaining potential ECIs. The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI.

A potential ECI which has passed through this procedure shall only be communicated to the Member States which may be significantly affected by the potential ECI.

Within a year from designating an ECI in the subsectors, Member States are to conduct an assessment of the threats relating to it. In addition, ***Member States are to report to the Commission every two years on the risks, threats and vulnerabilities the different ECI sectors are facing***. The need for additional Community measures to protect ECIs will be assessed on the basis of these reports.

To support the owners/operators of ECIs, the Commission provides access to best practices and methodologies regarding the protection of critical infrastructure. Furthermore, it supports the related training activities and exchanges of new technical information.

Any sensitive information regarding the protection of ECIs may be treated only by persons having the appropriate level of security clearance and only for the purposes the information was originally intended.

A European critical infrastructure contact point (ECIP contact point) is to be appointed in each Member State. Their purpose is to coordinate any ECI-related issues among Member States and the Commission.

8. The Protection of Critical Infrastructures in Romania

Romanian infrastructures are, almost entirely critical from at least a few essential viewpoints:

- They come from giant industrial infrastructures, inflexible, and un-adaptable to market economy, with traces yet to be liquidated;
- Romanian society and economy are in different stages of transition;
- Actions on the environment, massive forest exploitations, unorganized cultivation of fields, the lack of a coherent and efficient agricultural, ecological and environmental safety policy, generate dangers for critical infrastructure;
- The participation of Romania to the anti-terrorist coalition and other peacekeeping, crisis and conflict management missions can generate a new type

of threat towards citizens and vital economical, social and informational infrastructures as well as living conditions all together.

Of course, dangers and threats are much more numerous. They constitute the focus of a legislative initiative, and are included in the national security strategy, in the energy strategy program and other important documents, but are not yet fully overlooked, managed and controlled.

8.1. Promoting the concept

In Romania, notable steps have been taken at institutional level by the Romanian Presidency, Romanian Parliament (Defence, Safety and Public Order Commission of the Chamber of Deputies), Romanian Intelligence Service (supported by "RASIROM" Autonomous Company and Centre for Information on Security Culture - CICS) and in the framework of the Ministry of Economy and Finances, through the Security Structure of the General Directorate for Energy Policy and National Power Grid Company "TRANSELECTRICA" SA).

In the private sector, EURISC Foundation, Romanian Power Grid Company – TRANSELECTRICA S.A, UTI Group, RASIROM and recently ARTS - THE ROMANIAN ASSOCIATION FOR SECURITY TECHNIQUE had a major role in promoting the concept, organising series of round tables, national and international conferences, workshops as well running, as partners, research projects.

EURISC Foundation organized several events on the topic of critical infrastructure protection from the early stage this new concept started to be promoted by US and EU:

- The Ministry of Defence – The General Staff - hosted the ***Presentation by the EURISC Foundation*** of the "Clinton Report" regarding critical infrastructure (in 1997);
- The ***International Seminar on Risk Governance and Critical Infrastructure***, organized by EURISC Foundation, under the auspices of the President of Romania and with the participation of experts from the USA and Switzerland, as well as 200 civilian and military specialists from the Supreme Council of National Defence (CSAT) (in 2001);

- The ***International Seminar on Critical Infrastructure Protection***, organized by National Company "Transelectrica" SA and USAID (organized in 2003 in Bucharest);

- The ***International Seminar on Critical Infrastructure Protection***, organized by EURISC Foundation, under the auspices of the President of Romania. At the event took part experts from USA and Switzerland, and 150 civilian and military specialists from the Supreme Council of National Defence (CSAT) (in 2004)

- An ***International C.I.P. Seminar*** organized at the Palace of Parliament by the Defence, Safety and Public Order Commission of the Chamber of Deputies, in partnership with RASIROM Company, National Company "Transelectrica" SA and the Romanian Energy Regulatory Authority (ANRE), with the support of EURISC Foundation, UTI Group and Centre for Information on Security Culture (CICS) of the Romanian Intelligence Service) (in 2005)

- The ***International C.I.P. Seminar*** organised by National Company "Transelectrica" SA with EURISC Foundation, RASIROM Company, UTI Group, in partnership with "Reseaux Transport Electricité" (EDF) (organised in 2006 in Sibiu)

- The ***Roundtable on Critical Infrastructure*** of the Ministry of Economy and Trade, organised by National Company "Transelectrica" SA and EURISC Foundation (in 2006)

- In 2007 it was organised in Bucharest a ***Roundtable on Critical Infrastructure Protection*** by EURISC Foundation. At the event attended representatives of Romanian Presidency, National Company "Transelectrica" SA, RASIROM Company, UTI Group and others.

- In 2007 took place in Bucharest the ***International Seminar Critical Infrastructures Protection***, under the aegis of the World Security Forum. The event was organised by EURISC Foundation, with the participation of representatives of Romanian Presidency, Romanian Government, Ministry of Economy and Finances, Ministry of Foreign Affairs, National Company "Transelectrica" SA, RASIROM Company, ambassadors and diplomats, experts from USA, Norway, Greece and Romania, specialised in risk analyses and energetic critical infrastructure protection, focusing on energy security and the role of the transit countries. It was proposed to draft a regional security strategy, to organize an association of the transit countries and to launch a new concept of good energy governance.

With the aim to promote the implementation of European Program of Critical Infrastructure Protection in Romania, after 2007 to present were organised in Romania and abroad, by EURISC Foundation and above mentioned

partners: *5 seminars, 4 conferences, 6 workshops, 8 round tables, 2 NATO and EU experts meeting, 4 Public-Private Partnership National Forum on Security Sector, with topics on urban security and critical infrastructure resilience.*

Important step to promote the Critical Infrastructure Protection Concept in partnership with the Academy of Romanian Scientist and Polytechnic University Bucharest - The Power Engineering Faculty was made in 2009, 13 November, during International Conference on Energy and Environment (CIEM'09), given the opportunity to academia members, specialists from different sectors and students to present their research, opinion and proposal in relation with theoretical and practical aspects on critical infrastructure protection.

Also, Romanian experts from the Ministry of Economy, National Power Grid Company "Transelectrica" SA, Ministry of Interior and Administration and EURISC Foundation are part of European and Euro-Atlantic committees that promote the concept of critical infrastructure.

8.2. Specific legal framework in Romania

Institutionalization of the concepts is underway, and the notion of critical infrastructure is present in different legal documents, as:

- The National Security Strategy – document adopted by the Supreme Council for National Defence (Decision No. 62 / 17 April 2006);
- Government Decision nr. 2.288/9 December 2004 for the approval of the assessment of the main support functions offered by the ministries, other central governmental bodies and nongovernmental organizations on the prevention and management of emergency situations;
- Decision of the Minister of Economy and Commerce nr. 660/2004, on the approval of the Guidebook on identification of elements of critical infrastructure in economy;
- Decision of the Minister of Economy and Commerce nr. 791/2006 : on establishment of the « Working Group for the Protection of Electricity Critical Infrastructure»;
- Romania Strategy on Energy between 2007-2020, adopted in Mai 2007;
- The Law of National Security (Government Proposal), 2007;
- Romanian Government Decision No. 1489/09 September 2004 on establishing the National Committee for Emergency Situations;
- Romanian Government Ordinance No. 21/ 2004 on establishing The National System for Emergency Situations Management;

- Romanian Government Decision No. 1490/09 September 2004 on establishing the role and responsibilities for Emergency Situation General Inspectorate;
- Civil Protection Law No. 481 / 08November 2004;
- Other Government and Ministerial Decisions, harmonised with EU legislation, designed to protect their subordinated Critical Infrastructures and key assets.

Until further elaboration of new concepts, strategies, legislation and specific norms, specialized structures, dedicated logistics and allocation of financial resources for the functioning, endowment, training, simulations, exercises, security culture and information for the public, management of different types of emergency situations generated at the level of critical infrastructure is regulated through special laws (national safety, emergency situations, civil protection, etc) and the management is made through different permanent and temporary structures, organized at the level of ministries, departments, sectors and on specific domains.

Most of the intervention actions that are beyond the duty and possibilities of the sectors structures are carried out by the General Inspectorate for Emergency Situations (IGSU), subordinated to the Ministry of Interior and Administration, that formed the Inter-ministerial Group – Protection of the Critical Infrastructure, coordinated by the IGSU (2007).

By creating the Working Group at the level of the Ministry of Economy and Commerce (2006) the basis was established for a general framework for debates and decisions on the development of a coherent Energy Security Strategy a.o.

The Consultative Experts Group on Energy Security, established (2007) at the initiative of the Prime Minister of Romania, developed valuable points of view regarding energy sector critical infrastructure protection issues which were accepted included in the “Romanian Energy Strategy 2007-2020”

Participation in European projects within the framework of FP7 is a good opportunity to establish contacts with experienced partners from other EU member states and to have an expertise transfer on security research issues.

The Ministry of Education and Research of Romania, with the support of the Romanian Space Agency (ROSA), is organizing national competitions for financing projects on security research, a part of which are dedicated to the topic of energy security and critical infrastructure protection.

In Romania, in the framework of security research, over the last years, public-private partnerships were established and numerous subjects on the topic of

energy security and critical protection were debated (EURISC Foundation, National Power Grid Company TRANSELECTRICA S.A., RASIROM Company, UTI Group, a.o.)

At this stage, under Romanian Presidency National Security Department coordination, the Inter-ministerial Group – Critical Infrastructure Protection (initially formed in 2007 at Ministry of Interior and Administration), is working to elaborate and propose, taking in consideration the Directive EC 2008/114 requirements, the first Government Decision with the aim to establish the key issues relating to harmonize Romanian legislation with the new European Directive.

Conclusions.

☑ Current legislation, norms and regulations in force, as well as other regulations for specific sectors, with relevance for the community, previously issued, adopted, harmonized from a legislative point of view and published progressively in the Romanian Official Gazette starting with the year 2003, creates a database in the legislative field which will be taken into consideration by ministries and central administration, for promoting one legislative initiative that will define the Critical Infrastructure Concept in Romania.

☑ There will also be further work on designing work procedures, norms and standards for risk evaluation and analysis, information exchange between specialized structures, qualifications and responsibilities regarding guidance, control and coordination at central, ministerial and local or sectors level, (material and financial) logistics insurance as well as forces and ways for intervention.

☑ Romania's strategic options have in view the rapid development of some efficient and specialized infrastructure networks, **compatible with the European and Euro-Atlantic** ones, capable to amplify sustained development, as well as the accelerated modernization of the economy and the strengthening of national security. To this purpose, comprehensive programs of national investments will be launched, in cooperation and in partnership with other member states of the European Union and NATO.

☑ The Government, will aim to contribute with adequate measures to the improvement of national and international Critical Infrastructure Protection, through the development of a standardized methodology regarding the identification and classification of threats, ensuring adequate communication, coordination, efficient cooperation and coherent implementation of established protection measures with clear responsibilities for all subordinated structures with competence in this field, paying special attention to terrorist threats.

☑ Special attention will be paid to Energy and Transport Critical Infrastructures, considered as a sensitive domain with huge impact on national security, economic activity, citizen security, psychological impact on the population and loss of credibility of the Government and State administrative structures.

☑ In the field of energy, even if it has resources in operation, they are not sufficient to cover all the needs of its domestic market; thus, *Romania considers itself a transit country* with possibilities, but more importantly with responsibilities for assuring the security of the current and future energy transit routes to Western Europe.

☑ In this regard, Romania has the potential to involve itself actively at European Union Commission, Parliament and other structures, as well NATO level, for developing a common energetic strategy and for designing rules to be accepted by all partners in the relationship between producer, consumer and transit country.

☑ Romania is interested in having a good governance system in the field of energy, accepting the rules of the free market, as well as the need for intervention through a regulating mechanism for the transit of energy and trade, a real exchange of information in this field, the attraction and involvement of private partnership, of local communities and civil society in solving responsibilities that each one has in this domain.

☑ New international requirements in the area of Critical Infrastructure Protection and Energy Supply and Transport Security as well strong Cyber Security measures, at both NATO and European Union level, represent a requirement for Romanian national authorities for developing and implementing a coherent and unitary policy in this sensitive field of the contemporary world.

☑ EU Community members and NATO's expertise, international standards, as well as the legislation developed at the level of the European Union, represent the main sources for designing a new, long-term strategic vision for identifying, analyzing, assessing and managing national critical infrastructure, as well as for risk management and the improvement of the capacity to respond to threats.

☑ Knowing the interest of Romania to promote the security and stability in the wider Black Sea region, an important role can be attached to Romania's initiative that addresses mainly the issues of critical infrastructure, improving the regional cooperation in order to assure a normal functioning of the interconnected critical infrastructure, with priority being given to the transit systems for electricity, gas and oil, as well as air, railway, naval and terrestrial transport networks.

☑ In accordance with the major objectives assumed by Romania as regional factor of stability in a geographic area more and more subject to asymmetric risks, Romanian experts and other Romanian representatives actively participate in the specialized structures of the EU Commission and NATO Senior Civil Emergency Planning Committee (SCEPC). Thus, they have developed and participated also in other projects aimed at promoting the improvement of Civil Protection. A Memorandum of Understanding was signed with all neighbouring countries and bilateral projects were initiated with other European Countries as well with the United States Federal Emergency Management Agency (FEMA).

☑ Following EU and NATO integration many Romanian representatives, experts and specialists (military and civilian), well recognised in Europe and worldwide, are involved in different projects, European and international activities as experts or consultants in the field of Civil Protection as well as Critical Infrastructure Protection. We are proud that couples of them are coming with very important contribution on Energy Protection, Resilience and Mitigation or promoting new concepts on Risk Assessment and Mitigation for Interdependent Systems of Systems.

☑ At the same time, we would like to mention that the 2008 NATO Summit organized in Bucharest, offered the opportunity for approaching the issues of Critical Infrastructure Protection in general and energy security in particular, especially as a direct contribution of Romania to the security of each country, as well to the security of the North Atlantic Alliance in general. ***Bucharest Summit Declaration***, issued by the Heads of State and Government on 3 April 2008, highlighted the new NATO's approach to critical infrastructure protection, mainly "***NATO's Role in Energy Security",*** *as one of the* sectors having strong impact on allied nations defense capabilities.

REFERENCES

[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.