AES BIOFLUX
Advances in Environmental Sciences - International Journal of the Bioflux Society

Critical infrastructure protection in Romania. Evolution of the concept, vulnerabilities, hazards and threats

[1]Augusta-D. Gheorghiu, [2]Eugen Nour, [1]Alexandru Ozunu

[1]Babeş-Bolyai University from Cluj-Napoca, Faculty of Environmental Science and Engineering, Research Centre for Disaster Management, Cluj-Napoca, Romania; [2]"Gheorghe Pop de Băseşti" Inspectorate for Emergency Situations of Maramureş County, Baia Mare, Romania. Corresponding author: A.-D. Gheorghiu, adianacrisan@yahoo.com

Abstract. During the last years an increase in the number of events that affected vital infrastructures has been observed. The degree of interconnection between different systems and elements which are considered Critical Infrastructure makes them vulnerable to hazards and threats, which can have a natural, accidental or malicious nature. Due to this degree of interconnection, discontinuities in the operation or structure of any of the individual systems could jeopardize the integrity of the entire infrastructure system of a region or even nation. In these cases, one can speak about a true system of systems. Infrastructures are or become critical due to vulnerability, the direct threats against the system, or the actions and processes which they belong to. This paper is a brief review of the evolution of Critical Infrastructure protection in Romania, regarding the types of vulnerabilities, hazards and threats that can affect its integrity.
Key Words: Critical Infrastructure identification, Critical Infrastructure protection, vulnerability, hazards, threats.

Introduction. The concept of Critical Infrastructure (CI) has become a key subject in recent debates, with many international forums and publications dedicated to the subject. The current article aims to review the concepts and definitions currently used in the field, as well as the pursuits in terms of actions to identify and protect critical infrastructure elements in the European Union and Romania.

A characteristic of the systems which are considered to be critical infrastructure is their interdependencies with other systems, whether critical or not. For example, almost all systems characterized as CI use information technology which, in its turn, uses electricity. Due to these interdependencies, simple failures in one system can have dramatic consequences on other systems, rendering them temporarily inactive or inducing damages. As such, actions taken for the proper identification and protection of CI are of high importance.

Critical Infrastructure – concept, definitions and remarks. The literature defines critical infrastructure as including the following sectors: "information technology, telecommunications, energy, banking and finance, transportation systems, chemicals, critical manufacturing, agriculture and food, defence industrial base, public health and health care, national monuments and icons, drinking water and water treatment systems, commercial facilities, dams, emergency services, nuclear reactors, materials and waste, postal and shipping, and government facilities" (IJCIS 2012).

CI is determined by the ensemble of vital elements for the proper functioning of a society. The International Journal of Critical Infrastructures defines CIs on its website (IJCIS 2012) as ''networks for the provision of telecommunication and information services, energy services (electrical power, natural gas, oil and heat), water supply,

transportation of people and goods, banking and financial services, government services and emergency services".

As van den Bruggen (2008) remarks, this is a limitative definition, which covers ''infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defence or economic security", as described in a report for the US government (Moteff et al 2003). Cohen (2010) considers CI as something that people depend on, either directly or indirectly, in terms of life and wellbeing, in any timeframe.

The need to comprehensively define CI comes from the need to properly identify the elements and systems that constitute critical infrastructure. Since these elements and systems, as well as their good operation have crucial importance in times of war or conflicts, frequent assaults are planned on infrastructural systems such as power plants, airports or railways nodes, communication centres, etc. (van den Bruggen 2008). As such, their proper identification and protection becomes of great importance to Governments, in this case actions are taken by the European Union and countries worldwide.

Protection of Critical Infrastructure at European level. European Union Member States have taken actions to establish a common language and action plan regarding the protection of elements and systems of strategic value. The concern regarding the definition and security of CIs has been rising after the 9/11 events in the US and more stringently in Europe after the terrorist attacks of March 11th 2004 in Madrid, due to the necessity to fight this phenomenon of great extent worldwide.

In this regard, in June 2004, the European Council requested the European Commission to elaborate an overall strategy regarding the protection of critical infrastructure. As such, the communication regarding "Critical Infrastructure Protection in the Fight against Terrorism" was adopted on October 20th 2004, approaching aspects on the prevention, preparedness and response to terrorist attacks on CI. The conclusions of the Council on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" (EU Council 2004) validated the future proposal of the European Programme for Critical Infrastructure Protection (EPCIP). The Commission also agreed the set-up of a Critical Infrastructure Warning Information Network (CIWIN). Pursuant to this, a series of papers and communications concerning the protection of CI have been issued by the Commission, such as the Green Paper on a European Programme for Critical Infrastructure Protection, the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks" as part of the General Programme "Security and Safeguarding Liberties" (Council Decision 2007/124/EC), which aims to promote the assessment of risks to critical infrastructure and development of protection methodologies and security standards, as well as the encouragement of know-how and experience in protecting CI.

A notable action from the Commission in this field is the elaboration, upon a call from the Justice and Home Affairs Council, of a proposal for a Directive presenting the measures proposed by the Commission regarding the identification of European Critical Infrastructures (ECI) (COM 2006). In April 2007 the Council adopted the conclusions to the EPCIP, which specify also that the member states have the final responsibility to manage protection measures for CI within national borders, agreeing also that the Commission's efforts to elaborate a European procedure for the identification and designation of ECI are legitimate.

On September 2nd 2007, the European Commission takes the first steps towards the improvement of the CI protection, for the energy and transport sectors, adopting a communication through which the criteria that can be used for the identification of ECI in these fields are established (EC 2006). Precise criteria are meant to ease and harmonize the identification of CI in Member States, thus eliminating vulnerabilities. This communicate is the first sectorial approach in the implementation of EPCIP.

The Council Directive 2008/114/EC, on the identification and designation of ECIs and the assessment of the need to improve their protection, was enforced as of December 8th 2008. The Directive concentrates on the Energy and Transport sectors, and

will be updated to include other sectors in the field, technology of information and communication among others.

In the context of the Directive, a difference is made between CI for each Member State and ECI, as such (Council Directive 2008/114/EC):

- CI (in Member States): "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" (Council Directive 2008/114/EC, article 2, par. (a))

- ECI: "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". (Council Directive 2008/114/EC, article 2, par. (b))

As stated by the above-mentioned Directive, the primary and ultimate responsibility for protecting ECI belongs to the Member States and the owners/operators of such infrastructures. The Directive also specifies the need to have "Operator Security Plans ('OSPs') or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritization of countermeasures and procedures" (Council Directive 2008/114/EC, Annex II). Each Member State decides regarding the most adequate forms of action for implementing OSPs. Liaison officers identified for all designated ECI have the role of facilitating cooperation and communication between national authorities and European officials in the field of CI protection.

According to the Directive, the process of identification and designation of ECI was scheduled to end by January 12, 2011, and is to be revised periodically.

Protection of Critical Infrastructure in Romania. Romania, by the accession treaty to the European Union, signed on April 25th 2005, and the attached protocols, committed to transpose the entire Community acquis.

The National Development Plan 2007-2013, issued by the Romanian Government (PND 2005), establishes as a global objective the reduction, as soon as possible, of the socio-economic development difference between Romania and other Member States of EU and states the specific objectives of the process on 6 priority directions, which integrate, directly or indirectly the requirements for sustainable development on short and medium term. One of these priority directions, included in the National Strategy for Sustainable Development 2013-2020-2030 (GD 1460 2008), refers to infrastructure and its development, as well as the protection of critical elements of infrastructure.

In 2009, in a study conducted for the European Commission on the situation of CI protection activities across Member States (Booz & Co 2009) summarized the situation of Romanian actions and responsibilities regarding this matter as being mainly absent or inconsistent. Seven indicators were followed for the assessment of the status of CI protection in each Member State: Organizational Model, Strategy & Policy, Methodology & Standards, Public-Private Partnership & International Collaboration, Funding & Human Resources, Training & Exercises, and Sector-Specific Key Players & Initiatives.

Romania scored "not applicable" in the Methodology and Standards, Funding & Human Resources, Training & Exercises, and Sector-Specific Key Players & Initiatives fields, meaning that Open Source Research, Web-based survey and individual interviews have not shown information or data on the given argument. Regarding the Organizational Model and Strategy & Policy the study states that "there is no specific organization dealing with CI protection", "dealing in an unstructured way" with the matter, without any "specific strategies" for the protection of CI. Regarding the Public-Private Partnership & International Collaboration, the collaboration in the "development of the Mutual Support Integrated Operational System" for the relief of undesirable effects caused by natural or technological disasters and terrorist activities within the South-Eastern Europe region is noted.

Since 2009, when the above-mentioned study was released, the Romanian authorities have made progress in enforcing legislation and criteria for the identification and designation of CI, mainly due to the obligation to transpose the Directive 2008/114/EC by January 2011. As such, on November 3rd 2010, Emergency Ordinance no 98 regarding the identification, designation and protection of critical infrastructure was approved by Law 18/11.03.2011 (EO 98 2010). The Ordinance establishes the legal framework for the identification and designation of national and European CI on sectorial bases and the assessment of the necessity to improve their protection.

The sectors and subsectors pertaining to National Critical Infrastructure (NCI), as stated in EO 98/2010 and the public authorities responsible with their management are presented in Table 1.

The list of sectors and subsectors pertaining to ECI provided in the above-mentioned Emergency Ordinance and the respective responsible authorities at Romanian level are presented in Table 2.

The procedure for the identification of NCI/ECI is described in Annex 2 of EO 98/2010. The procedure resides in the application of sectorial criteria and critical thresholds (defined depending on the severity of the impact of the disturbance or the destruction of a certain infrastructure), as well as the application of inter-sectorial criteria:

- the criteria regarding *victims:* assessed depending on the possible number of deaths or harms;

- the criteria regarding *economic effects*: assessed depending on the importance of economic loss and/or the degradation of products and services, including subsequent environmental damages;

- the criteria regarding *effects on the population*, assessed depending on the impact of public trust, physical suffering or disturbance of daily life, including the loss of essential services.

These criteria are not cumulative for the identification of NCI/ECI, meaning that if either one of these criteria is fulfilled, the subject in cause could be designated as CI.

So far, sectorial criteria and critical thresholds have been established by legislation for 5 of the 10 sectors of NCI, as follows: Energy (Ord. 1178 2011), Information and Communication Technology (Ord. 4380 2011), Space and Research (Criteria 2011), Chemical and Nuclear Industry (Ord. 1177/4496 2011), Food (Ord. 5240 2011).

The critical thresholds for sectorial criteria are defined based on the severity of the impact of the disturbance or destruction of a certain infrastructure, and its unique character respectively.

According to article 11 of EO 98/2010, within 9 months of designating a certain infrastructure as NCI or ECI, the owner/operator/administrator of the NCI/ECI has the obligation to elaborate the Operator Security Plan (OSP) and send it to the responsible authorities for approval. The OPS identifies the critical infrastructure elements of the NCI/ECI and the existing safety solutions or the solutions which are to be implemented for the protection of the CI. The minimum requirements for the OSP are stated in Annex 3 of EO 98/2010, and include:

- the identification of important elements;

- the elaboration of a risk assessment based on major scenarios and threats, on the vulnerable points of each element and the potential impact;

- the identification, selection and establishment of priorities regarding countermeasures and procedures, making the difference between permanent safety measures, which identify the indispensable safety investments, and the means which are relevant for use in any situation.

Table 1

Sectors and subsectors of Romanian NCI and responsible authorities

No	*Sector and Subsector of NCI*	*Responsible public authority*
1	**Energy**	Ministry of Economy, Commerce and Business Environment
	Electrical energy, including nuclear	
	Oil and derived products	
	Natural gas and derived products	
	Mineral resources	
2	**Information and Communication Technology**	Ministry of Communications and Information Society;
	Communication systems, networks and services	Ministry of National Defence;
	Data processing and storage systems, including those of electronic public services	Ministry of Education, Research, Youth and Sport;
	Information security infrastructures	Service for Special Telecommunications;
	Communication systems and networks for the state cipher	Service of External Information;
	Radio and TV emission infrastructures	Romanian Information Service
	National postal services	
3	**Water supply**	Health Ministry;
	Drinking water supply	Ministry of the Environment and Forestry
	Water quality control	
	Damming and quality control of water	
4	**Food**	Ministry of Agriculture and Rural Development;
	Production and supply of food, ensuring food safety and security	National Sanitary Veterinary and Food Safety Authority;
		Ministry of Economy, Commerce and Business Environment
		Ministry of Education, Research, Youth and Sport
5	**Health**	Health Ministry
	Medical and hospital assistance	Ministry of Education, Research, Youth and Sport
	Medicine, serums, vaccines, pharmaceuticals	
	Bio-laboratories and bio-agents	
	Emergency medical services and sanitary transport	
6	**National security**	Ministry of National Defence;
	State defence, public order and national security	Ministry of Administration and Interior;
	Integrated system for state border security	Romanian Information Service;
	Defence industry	External Information Service
		Ministry of Economy, Commerce and Business Environment;
		Special Telecommunication Service
7	**Administration**	Ministry of the Administration and Interior
	Services and administration	
	Emergency services	
8	**Transport**	Ministry of Transport and Infrastructure
	Road transport	
	Railway transport	
	Airways	
	Shipping	
9	**Chemical and nuclear industry**	Ministry of Economy, Commerce and Business Environment;
	Production, processing, storage and use of chemical substances and nuclear and radioactive materials	Ministry of Education, Research, Youth and Sport
	Pipelines for hazardous chemical substances/products	
10	**Space and research**	Ministry of Education, Research, Youth and Sport;
	cosmic space	Romanian Space Agency
	research	

Table 2

Sectors and subsectors of ECI in Romania and responsible authorities

No	*Sector and Subsector of ECI*	*Responsible public authority*
1	**Energy**	Ministry of Economy, Commerce and Business Environment
	Electrical Energy	
	Oil	
	Gas	
2	**Transport**	Ministry of Transport and Infrastructure
	Road transport	
	Rail transport	
	Airways	
	Transport on internal shipping routes	
	Marine shipping on short distances and harbours	

Vulnerabilities, hazards and threads towards Critical Infrastructure in Romania. During the last years, the number of events which affected vital infrastructures has increased, because these infrastructure systems depend on each other. Discontinuities in the functioning of each of the systems could jeopardize the integrity of the whole infrastructure system. These can be considered a system of systems.

Nowadays, regardless of the development stage of modern societies, most threats to critical infrastructure present a certain degree of uncertainty. Under these circumstances, the risk model for critical infrastructures is not only dependent on the hazard, but also on the threat, critical elements and vulnerability, leading to the necessity of a systematic approach. This model was graphically expressed by the US Department of Defence (DoD 2002), as depicted in Figure 1.

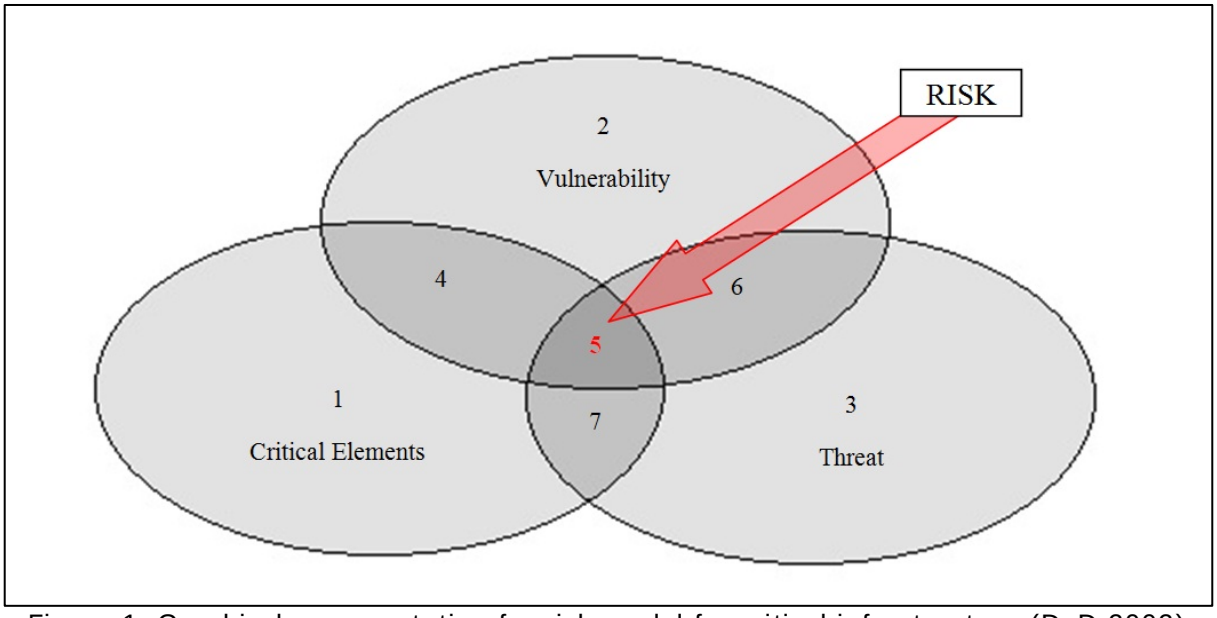

Figure 1. Graphical representation for risk model for critical infrastructure (DoD 2002).

The explanation for the numbers depicted in Figure 1 is as follows:

1. Critical elements (information, systems, programs, people, equipment or facilities) for which there is no vulnerabilities or threat exposures are known;

2. Vulnerabilities in systems, programs, people, equipment or facilities that are not associated to critical elements and for which no threat exposure is known;

3. Threat environment for which no threat to critical elements or access to vulnerabilities (or vulnerability information)is known;

4. Critical elements for which there are known vulnerabilities, but threat exposure is known;

5. Critical elements for which there are known vulnerabilities and threat exposure;

6. Threat has acquired specific knowledge and/or capability to exploit vulnerability although not a critical element vulnerability;

7. Critical element for which no vulnerabilities are known, but there is exposure to a specific threat.

Figure 1 one illustrates that threat and vulnerability alone do not determine criticality, which is determined by the simultaneous existence of the three factors. Usually, risk assessments are performed taking into account the occurrence probability of an event and the impact of that event, in terms of consequences. When it comes to critical infrastructures, the vulnerability of the element/facility considered needs to be taken into account in order to determine its criticality.

The assessment of vulnerabilities in correlation with critical infrastructures becomes more and more important, because of the stringent need to protect them against natural disasters, faulty technological exploitation, as well as disasters caused by the human factor, willingly or unwillingly, as well as other types of disruptions which can affect these elements. In the authors' opinion, vulnerability can be broadly defined as the result of the combination of existing risks for an entity with its capacity to survive and overcome internal and external emergencies.

Threats are mainly divided in two categories: physical threats (damage to the tangible property) and threats to the electronic/computer-based systems (cyber-attack) (DCSINT 2006). This classification was chosen because the computers and the connectivity computer systems brought to our lives and businesses, while increasing productivity and creativity, also increased vulnerability.

In Romania, the threats to the physical infrastructure are as much notable, as the vulnerability of this type of infrastructures has increased over the years due to inefficient or inconsistent upgrade measures regarding the physical integrity of the systems which constitute NCI (transport infrastructure, many industrial facilities and generally the built environment).

The combination of threats (hazards), vulnerability and consequences (expressed as a measure of economic loss, resources loss, etc.) results in risk, which in terms of CI and resilience can be assessed based on these three indicators. The total risk of a system is assessed as a combination, with the risk resulting from the assessment of all possible threat scenarios. The purpose of assessing the risk of a system is to be able to elaborate a risk management strategy which takes into account and recommends the application of countermeasures aimed at reducing the risk, usually based on a cost-benefit analysis. Factoring the cost for countermeasures in risk management strategies is an important aspect, as it has been noticed that even though the number of human life losses in case of disasters may have decreased during the last decades, the economic cost of disasters has increased significantly (Government of Canada 2003).

Types of hazards and threats to Critical Infrastructure in Romania. Some hazards and threats are intrinsic, such as system or process threats, as a result of the complexity and evolution of systems and processes (acknowledged as accidental threats). Others are issued on purpose, maliciously or as a result of certain interests. Other hazards and threats are simply natural, due to the environment hosting these CIs.

In this regard, hazards and threats towards CIs can be classified as follows: cosmic, climatic and geophysical hazards and threats, hazards and threats resulting from human activity, hazards and threats from the virtual space (Macuc & Predoiu 2008).

Cosmic, Climatic and Geophysical hazards and threats. These hazards and threats result, usually, from the physical dynamics of the Earth, meteorological and even cosmic phenomena. The most common ones are stated below (Macuc & Predoiu 2008):

- *Cosmic hazards and threats* towards physical critical infrastructure elements include: meteorite falls, intensification of solar and cosmic radiation, cosmic storms and other phenomena that can directly affect Earth;

- *Climatic hazards and threats* are much more frequent and numerous than cosmic ones, and they include hurricanes, thunderstorms, hail, heavy snowfall, extreme cold or

extreme heat waves, floods and flash floods, acid rain, extreme drought, etc. The extent of these hazards is large and often with sudden and chaotic variations;

- *Geophysical hazards and threats* result from the planet dynamics and include earthquakes, volcanic eruptions, tsunamis, landslides, land collapse, etc.

Hazards and threats due to human activity. Unfortunately, most hazards and threats which affect CI are due to human activity. These hazards and threats can be classified in two categories: intrinsic to human activity (i.e. human error) or unconventional confrontation means (malicious). Also, intrinsic human activity hazards and threats can be classified in 3 categories, based on their target: systems, processes or dynamics (Macuc & Predoiu 2008).

The main hazards and threats to CIs generated by *system malfunctions* are generated by the complexity of the infrastructure systems themselves, in their quality of metasystems or "system of systems". These types of hazards are numerous and difficult to avoid. Among these, we can mention physical and moral degradation of infrastructures, the evolution of some parts of the system which puts a strain on other parts (i.e. fiber optic leads traditional communication lines and other signal carriers to being obsolete), sudden collapse of part of the system (i.e. equipment malfunction) which leads to damage of other structures, boomerang effect, etc.

The hazards and threats specific to *physical and social processes* are the most complex and often extremely damaging. Among the most notable hazards and threats due to processes, the authors mention: changes in activities following various disturbance factors; economic, financial and other type of actions aiming at destroying competition; high-tech and IT innovations and different degrees of resisting to implement it; various malicious actions, including terrorism.

The hazards and threats caused by *dynamics* can include the actions mentioned above, but also many others which result generally from the philosophy and features of systems and complex dynamic processes. Among the most frequent the authors consider the sudden change in the functioning and behaviour of systems and their processes, rapid change in interlinks among systems, phenomena and processes due to internal, external or environmental changes, action of unpredictable disturbance factors, etc.

Hazards and threats to Critical Infrastructure in cyberspace. This type of hazards and threats usually target network lines, network nodes and vital centres, namely their physical equipment and systems (computers, servers, connections, etc.) as well as other infrastructure which harbour these means (buildings, power lines, etc.). In addition, these threats target databases and data storage and sharing facilities, or IT networks pertaining to companies, production lines, etc. All sectors of Critical Infrastructure are becoming increasingly interdependent, as cyber elements and telecommunications continue to support them. Critical Information Infrastructure and cyber infrastructure are susceptible to all types of hazards and threats: natural (i.e. destruction of infrastructure during natural disasters), accidental (i.e. malfunctioning due to aging equipment or overburdening, human error, etc.) but most often malicious.

It is easier to protect Critical Information Technology when it comes to physical security and physical assets. But when dealing with cyber-based threats, their capacity to create significant damage is readily available without needing high-end resources or exceptional computer science knowledge (Government of Canada 2003).

The factors which contribute to the vulnerability of Romanian Critical Information Infrastructure include four main aspects. First, the majority of the population which has access to this kind of infrastructure, the built environment and wealth is mostly concentrated in a few highly vulnerable areas, namely the largest cities of the country, and especially Bucharest. Second, the built environment of the country is already obsolete and is susceptible to damage from various hazards, and with natural disasters increasing due to climate change (third factor), this aspect becomes even more serious. The last aspect refers to communities highly reliant on advanced technologies which are frequently disrupted or damaged during disasters.

Conclusions. The protection of CI has become a priority in Member States of the European Union in recent years. This is due mainly to the increasing vulnerability of CI elements, thus making them more attractive to different threats. Romania makes no exception in this state of facts. The first step in protecting national CIs is to properly identify them. Even though a couple of years ago there were no practical measures in Romanian legislation regulating these aspects, matters are changing towards adopting clear criteria and thresholds for the designation of national and ECIs within the country borders.

Acknowledgements. This paper was realised with the support of POSDRU CUANTUMDOC "DOCTORAL STUDIES FOR EUROPEAN PERFORMANCES IN RESEARCH AND INNOVATION" ID79407 project funded by the European Social Fund and Romanian Government.

References

Booz & Co, 2009 Booz & Company (Italy) S.r.l., "Study: Stock-Taking of Existing Critical Infrastructure Protection Activities", Booz & Company Reference No: JLS-2007-D1-037_EU_CIP_StockTaking_Final_Report, available online at http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/2009_CIP%20stock_taking.pdf.

Cohen F., 2010 What makes critical infrastructures Critical? International Journal of Critical Infrastructure Protection 3:53-54.

DCSINT, 2006 Deputy Chief of Staff for Intelligence, Handbook No. 1.02, Critical Infrastructure Threats and Terrorism, August 10th 2006, Online at http://www.fas.org/irp/threat/terrorism/sup2.pdf.

DoD, 2002 US Department of Defense, Critical Infrastructure Protection, NDIA Information Briefing. July 3rd.

EC, 2006 European Commission Directorate General for Energy and Transport, Memo "Moving towards improved protection. Energy and transport infrastructure in Europe", available online at http://ec.europa.eu/dgs/energy_transport/security/infrastructure/doc/critical_infrastructures_memo_en.pdf.

Government of Canada, 2003 Office of Critical Infrastructure Protection and Emergency Preparedness, Threat Analysis. Threats to Canada's Critical Infrastructure, TA03-001, March 12th, Available online at http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/ta03-001-eng.pdf

IJCIS, 2012 International Journal of Critical Infrastructures, Inderscience Publishers, ISSN print 1475-3219, available online at http://www.inderscience.com/jhome.php?jcode=ijcis, last accessed December 2012

Macuc M., Predoiu C., 2008 Protection of critical infrastructures in the Euro-Atlantic space (Protecţia infrastructurilor critice în spaţiul euroatlantic). ANI Publishing House, Bucharest, 48 pp. [in Romanian].

Moteff J., Copeland C., Fischer J., 2003 Critical Infrastructures: What Makes an Infrastructure Critical? Report to Congress, Washington DC.

van den Bruggen K., 2008 Critical infrastructures and responsibility: a conceptual exploration. Safety Science 47:1137-1148.

*** Criteria, 2011 Sectorial Criteria of July 13th 2011 and subsequent critical thresholds for the identification of national critical infrastructures of the Space and Research sector, Official Gazette no. 530 of July 27th 2011.

*** COM, 2006 Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, Brussels, 12.12.2006, 787 (final).

*** Council Decision 2007/124/EC of 12 February 2007 establishing for the period 2007 to 2013, as part of the General Programme "Security and Safeguarding Liberties", the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks".

*** 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, Official Journal of the European Union, L 345/75.
*** EO 98, 2010 Emergency Ordinance 98 of November 3rd 2010 regarding the identification, designation and protection of critical infrastructure, Official Gazette, 757, 12.11.2010.
*** EU Council, 2004 Council of the European Union, Solidarity Programme on the consequences of terrorist threats and attacks, Brussels, 1 December 2004, available online at: http://ue.eu.int/uedocs/cmsUpload/15480EU_Solidarity_Programme.pdf.
*** GD 1460, 2008 Governmental Decision for the approval of the National Strategy for Sustainable Development – Horizons, Official Gazette, 824 of December 8th, 2008.
*** Ord. 4380, 2011 of June 6th 2011 on the establishment of sectorial criteria and critical thresholds for the identification of national critical infrastructures of the Information and Communication Technology sector, Official Gazette, 847, of November 29th 2011.
*** Ord. 1177/4496, 2011 Order for the establishment of sectorial criteria and critical thresholds for the NCI sector National Critical Infrastructure „Chemical and Nuclear Industry", Official Gazette, 581, of August 17th 2011.
*** Ord. 1178, 2011 Order of June 6th 2011 for the establishment of sectorial criteria and critical thresholds for the sector of NCI/ECI National/European critical infrastructure – "Energy", Official Gazette, 436, of June 22nd 2011.
*** Ord. 5240, 2011 Order of August 30th 2011 (Ord. 5240/2011) for the establishment of sectorial criteria and critical thresholds for the NCI sector – National Critical Infrastructure - "Food", Official Gazette, 691, of September 29th 2011.
*** PND, 2005 The 2007-2013 National Development Plan (Planul National de Dezvoltare), Romanian Government, Available online at: http://discutii.mfinante.ro/static/10/Mfp/pnd/documente/pnd/PND_2007_2013.pdf.

Received: 20 February 2013. Accepted: 25 February 2013. Published online: 15 April 2013.
Authors:
Augusta-Diana Gheorghiu, Babeş-Bolyai University from Cluj-Napoca, Faculty of Environmental Science and Engineering, Research Centre for Disaster Management, 30 Fântânele Str., 400294, Cluj-Napoca, Romania, e-mail: adianacrisan@yahoo.com
Eugen Nour, Inspectorate for Emergency Situations "Gheorghe Pop de Băseşti" of Maramureş County, 87 Vasile Lucaciu Str., 430322, Baia Mare, Maramureş, Romania, e-mail: eugen.nour@yahoo.com
Alexandru Ozunu, Babeş-Bolyai University from Cluj-Napoca, Faculty of Environmental Science and Engineering, Research Centre for Disaster Management, 30 Fântânele Str., 400294, Cluj-Napoca, Romania, e-mail: alexandru.ozunu@ubbcluj.ro

How to cite this article:
Gheorghiu A.-D., Nour E., Ozunu A., 2013 Critical infrastructure protection in Romania. Evolution of the concept, vulnerabilities, hazards and threats. AES Bioflux 5(2):148-157.