# The Economic Value regarding the Protection Activities of Critical Infrastructures

**Valentin-Bogdan DĂNILĂ**[1]

**Abstract:** In the past two years, a number of European countries, members of EU, Australia and Canada have initiated substantive actions in PIC area, establishing bodies responsible, defining procedures and methodologies, allocating significant resources to protect critical infrastructure considered essential or vital. The security concept, and implicit, the economical and energetic ones have different use and defining in relation to the history and organizational culture of every nation. A decisive contribution in the process of defining those concepts is identifying the set of values and national interests, elements that usually are the result of the public opinion perception. The increased share of non-military risks and threats has determined the national security management reconsideration, becoming more obvious the necessity of "public-private partnership" approach. A new concept is becoming more and more present and gains maximum generality significations. This kind of process reconfigures the position and the role of social state actors: the political class, the business and scientific environment, civil society and citizens.

**Keywords:** critical infrastructures; national security; vulnerabilities; treats; risk analysis

## 1. Introduction

The international security environment, that includes the security of our nation is presenting more and more obvious alterations from the perspective of new risks and threats, apprehending the increase of non-military, and also economical, financial, banking, religious and information aggressions.

The security of a nation, according to the "European Security Strategy" is defined by five dimensions: political, military, economical, diplomatic and environmental protection.

Conformably to the European Union, the security management represents "*a deliberate process by whom is endorsing the risk valuation and spreading actions meant to bringing it to a determined and acceptable level, with an acceptable price*".

[1] Senior Lecturer, PhD in progress National Academy of Information "Mihai Viteazul", 20-22 Odăi Road, Sector 1, Bucharest, Romania. Tel.: +40.0237/214041. Corresponding author: danila.valentin.bogdan@gmail.com.

Security management hints at:

- identifying the risk associated to the critical infrastructures of system and process vulnerabilities, dangers and threats,
- the analysis and risk valuation
- the control of its dynamic
- maintaining it to the established limits

"*A nation is secure if reproducing and functioning and so is being capable of revaluating the products of interrogative processing, in domains and rhythms which ensure the required adaptability in internal or international social evolutions, competitiveness in relevant domains, the capability of identifying social aggressions - no matter of their nature and source - and if produced, to counteract them in ways which don't affect its reproduction capacity*." (Toba, 2003)

Obviously, economical security is the one generating security resources and as part of it, energetic security is an essential premise of normal state function and the wellbeing of its citizens.

To defining those notions one of the characteristic stages is the valuation and risk analysis, process which nowadays constitute complex analysis subjects and theoretical and methodological reconfiguration, in national and international levels. This measure finality is defining "critical infrastructures" and identifying the most adequate modalities to protect them.

General William L. Nash, during a conference in Romania in 07 October 2006 said that "*it is important to have people thinking of the future. But at the same time it is difficult to make predictions. So, we can't always know what is going to happen. Meanwhile, I think it is important, for the government, for the academic institutions to look towards the future, to define trends. For example, I think that in the next decade the demography will have a very important impact on the civilization. We are confronting nowadays with phenomena like radicalism or terror which purpose is promoting some persons ideas, ideologies. It's a new world we are confronting downright. This is why our politicians are enough confused. It is like someone is moving the wire when you are trying to keep your balance, and every time you get used to the vibrations, it changes the wave vibration. It is very difficult and dangerous. Regarding your political situation and state strategy, you have to keep*

*in consideration the politicians challenges, governmental leaders and you have to treat equally the future issues, no matter which political forces are in charge."* [1]

## 2. Conceptual Details

In a study by the Centre for Defence and Security Strategic Studies, National Defence University in Bucharest, entitled "Critical Infrastructure. Danger, threats to them. Protection Systems ", authors D. Gheorghe Alexandrescu and D. Vaduva Grigore approach CIP issues from systemic perspectives.

According to the authors we can distinguish, in relation to location, role and importance for the stability and functionality of systems, their security, the following classes of infrastructure:

1. Normal Infrastructure – NI;
2. Special Infrastructure – SI;
3. Critical Infrastructure – CI.

By special infrastructure, we allow those that are high performance. Critical infrastructures are usually a determining factor in the stability, safety and security systems and processes, having an important role in ensuring safety in the operation and performance of economic, social, political, and military processes.

The authors, renowned military analyst, believes that C.I. is "a commodity that is vital to the functioning of the economy and society" (Alexandrescu & Văduva, 2006, p. 12) and through CIP we can accept "all measures established to reduce the risks of blocking the operation or destruction of critical infrastructure." (Alexandrescu & Văduva, 2006, p. 12)

Regarding the CIP two hypotheses are supported:

1. is impossible to achieve total protection;
2. there is no generally accepted model.

The term "critical infrastructure" was used officially for the first time in July 1996 when the U.S. president declared the "Critical Infrastructure Protection Executive Order." In accordance with the "Preamble" of this document: "Critical infrastructures are part of national infrastructure, which is so vital that the

[1] http://www.ziua.ro/display.php?data=2006-10-07&id=208710.

destruction or making it incapable of functioning may seriously diminish the defense or the U.S. economy."

The document stated that C.I. family includes:

- telecommunications;
- electricity and water supply systems;
- gas and oil deposits;
- banking system;
- emergency services;
- continuity of government.

Infrastructures are considered critical because:

- a unique condition in the infrastructure of a system or process;
- the vital importance that they have, as material or virtual (network) support in the operation and performance of economic, social, political, informational, military processes;
- the important role that is irreplaceable, which fulfil the stability, reliability, safety, functionality and, especially, in security systems;
- increased vulnerability to direct threats, as well as those aimed at systems in which they belong;
- the particular sensitivity to the variation in conditions and, especially, in sudden change of situation.

Presidential Commission on Critical Infrastructure Protection (1996) in the U.S., said that the nation's security, economy and survival of the industrialized world depends on:

1. electricity;
2. communications;
3. computers.

The evolution of society, led reconsidering the reference range and the "National Strategy to Secure Cyber Space" (2003, USA) proposed the following definition of CI: "*Public and private institutions in the agricultural, food, water supply, public health, emergency services, defence industries, information and telecommunications, energy, transport, financial and banking, chemical and hazardous materials areas, as well as postal and navigation.*"

According to the definition accepted by NATO, C.I. are those: "*Facilities, services and systems, which are so vital to the nation, that their removal or destruction may*

*have destabilizing effects on national security, economy, population health and effective functioning of government*."

C.I. Protection includes "programs, activities and actions by governments, owners, operators and shareholders to secure this infrastructure." "Senior Civil Emergency Planning Committee" in NATO, has appointed eight subordinated committee to identify the solutions for to the unitary identification to problems connected to CI defining criteria, for models and methods of risk analysis and risk identification and also methods of their protection. Critical infrastructures from the EU include: "physical and information technology facilities, networks, services and assets in case of stopping or destruction, may cause serious incidents on the health, safety or economic welfare of citizens or governments of Member States activities."[1]

Critical infrastructure, according to European Commission document, includes:

- plants and networks in the energy sector (especially electricity generation plants, oil and gas refineries and storage facilities, transmission and distribution systems);
- communication and information technologies (telecommunications, broadcasting systems, software, all data and networks, including Internet etc.).
- finance (banking, securities and investment markets);
- health care sector (hospitals, care facilities for patients and blood banks, laboratories and pharmaceuticals, emergency services, search and rescue services);
- food (security, means of production, distribution and food processing industry);
- water supply (reserves, storage, treatment and distribution);
- transportation (airports, ports, intermodal facilities, railroads, mass transit networks, traffic control systems);
- production, storage and transport of dangerous goods (chemical, biological, radiological and nuclear);

Council of Europe (June 2004) asked the European Commission and the High Representative to develop a global strategy on strengthening and protection CI. It was submitted a new definition of CI, as they are: "Information technology and physical facilities, networks, services and activities, which, in case of stopping or

[1] http://europa.eu.int/eurlex/lex/LexUriServ/site/fr/com/2004/com2004_0702fr01.pdf.

deterioration, can produce serious incidents to health, safety or economic welfare of the citizens or Governments of Member States activities."

European integration, amid the current interdependence, generates increasing vulnerability gradient of CI from EU Member States. According to the European Commission may be accepted three essential criteria for identifying CI, as follows:

1. length or surface;
2. degree of seriousness - incidental (zero, low, moderate or high), economics, the public domain, the environment, etc.;
3. effect over time - the time after which they become major or serious consequences.

## 3. Typology of Critical Infrastructure

Studies show that infrastructures become critical in place and the powers of the system by determining the stability and reliability of the system, the exposure to wear degree and disturbance, by family with variable geometry of vulnerabilities (system, process or induced). Some specialists consider that an infrastructure or component is considered critical in relation to its strategic position in embedded systems and, more generally, in relation to the interrelationship which is related to other components or infrastructure. Systemic approaches are appropriate to CIP. In terms of spatiality to which they belong, the CI can be defined as:

1. critical infrastructures from physical space;
2. critical infrastructure from space;
3. critical infrastructure from cyber space.

Their degree of interdependence increases greatly with the evolution of life on earth and those who hold political systems, economic, financial, social, informational, cultural and military reinforces in globalization stage, becoming an essential feature of them. This feature, logically, should increase the coefficient of completeness of all facilities and restricting the crowd of critical infrastructure only to those which determines the stability and functionality of the system.

Unfortunately, things, at least for a foreseeable future, are not so. Interdependence and structures completeness creates a whole new kind of vulnerability that we will call, generically, vulnerabilities of completeness or vulnerabilities of interdependence. For example, the integration of all global airlines, although automatically lead to increased traffic, transport speed, compressing both, both

time and space, should also lead, automatically, to the reduction functionality and stability vulnerabilities and increasing transport efficiency, which, moreover, happens. At the same time, however, airlines are integrated on a planetary level extremely vulnerable to terrorist attacks, the calamities and disasters and other risks and asymmetric threats.

Physical infrastructures are always supports of physical systems, usually from the area of human society, with function and social roles. So, they can be grouped into categories of physical systems, as follows:

**Enterprise's critical infrastructures**: electric power distribution network of 380 volt or high voltage, industrial water distribution network, computer network, distribution of natural gas, fuel or other substances and materials are absolutely necessary for production, network communication (command control), network storage of raw materials and finished products, the physical network computers, computers, cables, connections) etc.

**Critical infrastructure of sector (industry**): water distribution, electricity, natural gas used in the production process, strategic materials from businesses and the branch, special material storage network (strategic materials, flammable materials, radioactive materials, substances chemical, biological agents and other high-risk) communication networks, especially their physical infrastructure (relays, cables, stands, stations etc.) road and rail networks: car parks, physical networks of computers; data bases and other vulnerable elements or with important role in the functioning of businesses and institutions.

**Critical infrastructure of the economy**: infrastructure of strategic road networks, especially railway hubs, networks of production and distribution (national energy system infrastructures), infrastructure management systems, and networks of strategic materials deposits, raw materials, chemical, nuclear or biological agents.

**Air transport of critical infrastructures**: airports, energy supply systems, water, gas, fuel storage networks, parks and aircraft hangars, control towers, air traffic control infrastructure, computer networks, radar stations, stations routing the landing, other infrastructure systems that depend on flight safety and security.

**Critical rail infrastructure**: the railways, bridges, viaducts and works of art on or adjacent track, stations, electrical networks rail transport, communications networks, and other types of networks.

**Critical infrastructure of shipping**: ports, port infrastructure plays an important role, unique and irreplaceable in the operation of ports and marine transport, plant lamp, radio navigation stations, radar stations, communications systems, networks and major roads, railways inside the port, pier protection systems, other infrastructure systems security and safety of navigation on the seas and rivers;

**Critical infrastructure of the financial system**: banks' offices, media information, computers, systems of protection and safety of transport networks and ATM interchange of money, deposits.

**Housing critical infrastructures**: electrical, gas and water, home security systems.

**Critical village infrastructure**: water electricity and gas transport networks, especially buses, checkpoints and the distribution, public transport networks (subway lines, trolley lines, buses and trams, some buildings and various other important related works), telephone networks, relay stations and central relays and radio and television stations that are national or local system alert, public lighting; heat supply, wells, pumping stations and other infrastructure of water purification systems, hospitals and other infrastructures of emergency medicine and emergency care, laboratory and hematology centers, infrastructures operating rooms, recovery rooms and other compartments surveillance and monitoring of patients in need, infrastructure systems and fire prevention, civil protection infrastructure systems, particularly systems and networks for action and response to disasters, disasters, nuclear accidents, industrial, chemical and technological networks and warehouses, etc.

**Critical infrastructure of the province (county, area etc.)** Railways and major public roads, especially the vital centers, or nodes, stations, depots, communications centers, etc.; network storage, pipelines, telephone networks, relays microwave communications systems, art works, dams, water reservoirs, sewage systems with vital impact on the cultivated or inhabited lands, dams and other infrastructure control floods and overflows, deposits network of local, regional or national importance, elements of national or international critical infrastructure, special infrastructure.

**Critical infrastructures in the country**: the national network infrastructures of energy (energy units, power lines, transformer stations, installations and systems for monitoring and control, hydro-power dams and reservoirs, nuclear power systems of these nuclear facilities , hydro and thermal power plants, heavy water

plants, deposits of raw materials, hazardous materials and strategic materials etc.) road network of national or international; vital infrastructure of these networks, railway network with all related structures (stations, depots, rail networks supply of electricity, rolling stock, fuel and other materials vital command control systems and traffic control, infrastructure of railway communication systems, etc.) national air transportation network, with all the infrastructures, vital elements of international air traffic network in the territory of the country, the naval transport infrastructure (ports, port facilities, dams, navigation safety infrastructure , coastal zone infrastructure, facilities and infrastructure HA, radiophone and other signaling systems); the national communications infrastructures, but also other systems of national and international communications (telephone networks, central communications hubs of these networks, transport equipment, optical fiber routes, relays, signal modulators etc.) physical infrastructure of national information networks, computers, television etc. national infrastructures alert networks and gas pipelines as part of national or continental transport networks etc.

**Military critical infrastructure**: military communications network at the strategic and tactical level, these network infrastructures, facilities for military aerodromes, the military ports, military bases and other locations, networks, pipelines, depots and fuel supply systems , ammunition, food and essential supplies products both in peacetime and in war or crisis management process and participation in armed conflict, roads, rail and naval, network of warehouses, arsenals, computer networks, computer systems.

**Critical infrastructure of the system of public policy**: the police and gendarmerie facilities, infrastructure of the fire fighters and emergency Inspectorate; infrastructure of rapid reaction forces and formations, critical infrastructure protection system of the citizen, property and institutions.

**Critical infrastructure information system and state security**: intelligence infrastructure and other institutions that depend on data protection, national and alliance interests, values and heritage;

**Critical infrastructure of the health system and protection the citizen, family and community**: hospitals, emergency networks, laboratories, drug stores, infrastructures, etc. medical research centers.

**Critical infrastructure of space** includes orbital stations, satellites, space communications systems etc.

**Critical infrastructure in cyberspace includes**: cyberspace, critical infrastructure, critical infrastructure of communications systems, critical infrastructure of networks and databases.

## 4. National Critical Infrastructure Protection

Romanian national critical infrastructure protection is included, in one form or another, the European Program for Critical Infrastructure Protection in at least three ways:

- adapting the system of law, action and emergency response to European requirements in preparing integration and the proper integration;
- critical infrastructure dependencies and interdependencies of the Romanian and European;participation in the development and implementation of policies and strategies to combat terrorism, illegal traffic, organized crime and asymmetric threats.

Critical Infrastructure Protection (CIP) entails, for the achievement of performance standards, a clearly defined partnership between:

1. IC owners;
2. operating personnel or management;
3. competent authorities.

Can be identified three approaches to CIP, as follows:

- critical information infrastructure protection, which concern only the security of IT connections and solutions to protect them, the powers for the other families of IC being diverted from other public or private;
- it takes into account both IT networks and the physical elements of the CI, approach in which physical protection is a component of the national civil defence system and focus on cooperation between public and private sector (if it is taken into account all risks - "All Hazards approach");
- a less widespread approach and only focuses on the protection system of government and certain state institutions.

In a study by George Dediu, Central State Office for Special Problems of the Romanian Government entitled "Critical Infrastructure Protection - a new challenge", an alternative approach to advancing the PIC in seven stages, as follows:

**1. Sector Analysis** - Defining the critical sectors should be carried out by joint groups of experts from government, private sector, managers and specialized

agencies in protecting the physical and informational. In accordance with the experience of other countries in the EU and NATO the following sectors can be considered critical areas: banking system, government system, telecommunications, transport, energy (electricity and fuel), health, emergency and rescue services and supply water.

**2. Interdependencies Analysis** - determination of interdependencies is based on identifying vital processes and their essential components of the system, while defining the nodes and relations with other systems.

**3. Risk Analysis** - involves the approach in which are determined the probabilities of events and the consequences thereof, to determine appropriate procedures for implementing the decisions in this area. In summary this stage will attempt to answer three questions: what are the emerging adverse events? Which is the probability of them? Which are direct consequences thereof? The objective of this phase is the identification, quantification and risk assessment. The purpose of the approach is to achieve an effective management of risks.

**4. Analysis of Threats -** a threat can be represented by an individual, organization or nation and will include determination of: the nature of the threat (internal or external), the source and occurrence.

**5. Vulnerability Analysis** - Vulnerability can be defined as a characteristic of the architecture, implementation or operation of a system that includes CI, which it is exposed to destruction or disturbance. Identify vulnerable areas and the consequences of these facts are assessed by quantification (insignificant, minor, major, and high-catastrophic).

**6. Analysis of the Consequences** - such an approach is the prerogative of experts and it may be qualitative or quantitative, each variation offers advantages and limitations.

**7. System Analysis** - if we admit that the system is a complex infrastructure, a simple infrastructure, an infrastructure dependent entity, or a system embedded in infrastructure, according to four levels of hierarchy: system of systems, individual infrastructure, system individual or business and technical components. In this last step we use modelling and simulation to determine interdependencies.

Romanian vital infrastructures are almost entirely critical infrastructure from at least a few main reasons:

- they come from the giant-economy infrastructure, inflexible and difficult market adaptable economy, whose traces have not yet been liquidated or improved;
- Romanian economy and society as a whole, is in a state of chaos, specific to long and repeated periods of transition, where everything or almost everything is vital, critical and vulnerable;
- indiscriminate actions on the environment, massive cutting of forests, chaotic land cultivation, agricultural disaster, lack of agricultural policy, ecological and environmental protection, consistent and effective, creates very serious threats at all and especially on the critical infrastructure.
- is expected that participation of Romania in the antiterrorist coalition and other missions of crisis management and conflict resolution and peacekeeping, to generate a new kind of threat to the citizens and vital infrastructure of the economy, society, information and living conditions.

Of course, dangers and threats are more numerous. They are subject to legislative initiatives are included in the national security strategy and other important documents, but are far from being fully monitored, managed, controlled and removed.

## 5. Conclusion

Analyzing the requirements of the Green Paper on the European Program for Critical Infrastructure Protection "we can advance some views, as follows:

- terrorist attacks in recent years allow us to advance the idea of a renewing of the notion of "critical infrastructure" in the "critical networks";
- as a direct approach is preferable in the financial synergy protection measures, targeting not only be, for example, the economic;
- if a framework is chosen it should be accompanied by a system of sanctions, which is difficult to implement if, for example, a State does not make a CIP according to procedures;
- the development of a European reference system will allow a hierarchy within states and at European level, the CI;
- there is an urgent need to undertake a coordinating authority to ensure the coherence of the European system;

- the coordinating authority will be "grafted" on an existing institution to save time and resources (this is the case in Romania where it set all kinds of agencies and authorities not to maximize the potential of existing institutional structures).

## 6. Bibliography

Alexandrescu, G. & Văduva, G. (2006). *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie/ Critical infrastructure. Danger, threats to them. Protection Systems*. Bucharest: Universităţii Naţionale de Apărare „Carol I".

Patriciu, V.V.; Petroşanu, M.; Bica, I. & Cristea, C. (1998). *Securitatea informatică în Unix şi Internet/ Computer security in Unix and Internet.* Bucharest: Tehnică.

Wenger, A.; Metzger, J. & Dunn, M. (2002). *The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries.*

Wenger, A.; Metzger, J.; Dunn, M. (2004). *The International CIIP Handbook: Evolution of the Critical Information Infrastructure Protection (CIIP)*.

Toba, F. (2003). *Decizia politică şi securitatea naţiunii/ Political decision and national security.* Bucharest: Licorna.