OVERVIEW OF CRITICAL INFRASTRUCTURES PROTECTION IN ROMANIA

Marius Laurentiu ROHART

Abstract

Technological developments and globalization have created new interdependencies between the systems that are vital for societies' well-being: its critical infrastructures . If previously countries were preoccupied with the early, local infrastructures such as transportation or communication, today's modern societies work with fast, global and digital connections in all major infrastructures - from energy distribution and finance to public health. This highly evolving context brings new challenges (both threats and opportunities) that shape the way security and stability of critical infrastructures should be ensured at national and international level. This paper aims to offer an overview of Romania's status on the protection of its national critical infrastructures, as well as its relation to international initiatives on this topic. It does so by analyzing the definition of critical infrastructures and how they evolved in particular international contexts, as well as as the unique characteristics of the Romanian context.

Keywords: *Romanian critical infrastructure, European critical infrastructure, national security, security crisis management, CCPIC, physical threats, cyber attacks, critical infrastructure management, critical infrastructure protection.*

Chapter 1: About (inter)national critical infrastructures

1.1 Defining critical infrastructures

A country's critical infrastructures are the specific facilities, services and informational systems that are vital to its national security, economy, public health, and for the security and well functioning of the Government itself. The failure or destruction of such critical infrastructures could heavily weaken or threaten the latter. As such, both the management and protection of critical infrastructures go hand in hand.[1]

Each country is responsible for identifying the national infrastructures that are critical for its security and stability. However, there are certain infrastructures deemed critical by most states.

Which are Romania's critical infrastructures then? They fall into the following major categories: the production and distribution of electricity, production and distribution of oil and gas, telecommunications, the financial system, transportation, water management, medical emergencies, and the continuity of Government activities. More concretely, these infrastructures can take the form of pipe networks (for distributing water, gas, petrol), wired networks (for telecommunications, electricity, Internet), dedicated networks and databases (for financial industries or military organizations), roads, airports, harbours, nuclear plants etc.

[1] Steiner, Nicolae. Andriciuc, Radu. *Infrastructura critica. Vulnerabilitatile si protectia ei.* Bucuresti, 2010. http://www.academia.edu/4377219/Consid_priv_protectia_infrastructurii_critice

How can these critical infrastructures be subject to attack, failure or weaknesses? Threats can be either physical or virtual. For example, an earthquake or a heavy storm are physical threats that affect electricity (by causing electrical surges) or transportation (by blocking roads and people). Cyber attacks are virtual but can nevertheless heavily affect the control and management of telecommunications, electricity and finance to name a few (for example, by causing IT failures affecting financial transactions).

Critical infrastructures can also be defined in opposition to ‘common infrastructures’ and ‘special infrastructures’.[2] Common infrastructures are the foundations of any system - for example roads, schools, local authorities, factories and nuclear plants etc. Special infrastructures have the role of enhancing the performance of various national systems (i.e. by modernization, increased security). Any of these latter types of infrastructures can be named critical in the sense that if they are subject to damage the integrity of the overall system to which they belong is compromised - the case of roads that connect various countries, should territorial conflicts arise, or if a nuclear plant becomes subject to attacks.

It is important to note that infrastructures are not critical in themselves, but that accurate analysis needs to be carried on all infrastructures in order to identify those of significant importance. Critical infrastructures are called as such because[3]:

- they are unique amongst other systems and infrastructures
- they have a vital input on the functionality of other systems and infrastructures
- they cannot be replaced in their role for assuring the security and functionality of other systems and infrastructures
- they are particularly vulnerable to internal and external conditions and can be threatened or attacked.

Critical infrastructures can be physical (roads, wires, pipelines, etc), cosmic (satellites and orbital stations) and virtual (virtual telecommunication systems, networks, databases). Computer networks are particular in this respective sense, as they entail both physical and virtual side.

Through technological developments, currently most critical infrastructures depend on IT networks and software, making one industry interconnected and interdependent with the others. However, this also means that a failure or weakness in one of them can easily translated to others. In other words, a problem affecting the telecommunications industry will surely reflect in the financial system too.[4] The 9/11 terrorist attacks on World Trade Center led not only to loss of lives but also to shortages in electricity, transportation halts, communication failures and severe drop in global stocks on stock markets.

To prevent this from happening in the future, the main aim of today’s strategies for critical infrastructures protection is to make public and private actors within this field work in local, national and international partnerships in order to be better prepared in preventing, analyzing and solving potential threats.

1.2. The origins and evolution of the term ‘critical infrastructure’. International approaches.

[2] Alexandrescu, Grigore. Vaduva Gheorghe. *Infrastructuri critice. Pericole, amenintari la adresa acestora. Sisteme de protectie*. Editura Universităţii Naţionale de Apărare „Carol I”. 2006. http://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf

[3] Idem 2.

[4] Wikipedia http://en.wikipedia.org/wiki/List_of_stock_market_crashes_and_bear_markets

The term ‘critical infrastructures’ began to be used in 1980s in the United States, where a history of attacks and threats on the country’s values and objectives have led to the inauguration of the Presidential Commission for the Protection of Critical Infrastructures. It initially focused on three main industries: electricity, communications and computers. However, following the increase in terrorist attacks such as the 1993 World Trade Center bomb attacks and the 2001 fall of the twin towers led to the United States proposal that an international partnership should be agreed upon in order to collaboratively face globalized vulnerabilities and attacks. At the end of 2001, the US launched the Executive Order for the Protection of Critical Infrastructures. Two years later, the US tackled cyber security too with the National Strategy of Securing the Cyber Space, where it expanded the notion of critical infrastructures to include water and food management, public health, medical emergency responses, national defence, chemical and toxic substances management etc.[5] This lead to international agencies such as NATO and the EU to also acknowledge the importance of such critical infrastructures and of partnerships for securing them.

For the European Union, this became a top priority following terrorist attacks such as those in Madrid (2004) and London (2005), which lead to the immediate call for global strategies in protecting critical infrastructures[6]. In 2004 the EU had already established the European Programme for Protecting Critical Infrastructures and in 2005 it launched CIWIN - Critical Infrastructure Warning Information Network in order to foster communication and warning disseminations to all its member states.

These initiatives and many others eventually led to a concrete legal framework - the well-know directive 2008/14/CE[7]. The directive requires all EU member states to develop internal legislation and delegate specific institutions that can effectively protect their national critical infrastructures. The directive has a strong focus on collaboration between member states, as one’s national infrastructure can easily impact another’s. This way, the EU acknowledges that physical borders are less relevant when discussing critical infrastructures, with globalization making them highly technologized and interdependent; as such, new partnerships must be formed in order to effectively tackle potential threats.

Chapter 2: Critical infrastructures protection in Romania

2.1 Legal framework in Romania

Romania responded to the European Union and its Directive 2008/114/CE[8] that proposed all EU members to develop legislation and activities that would identify, manage, develop and secure critical infrastructures on their territories.

Romania first launched the emergency ordinance OUG number 98/2010[9] that was later approved into legislation as law 18/2011[10].

[5] Idem 2

[6] Serviciul Roman de Informatii. http://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf

[7] Comisia Europeana. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm

[8] Centrul de Coordonare a Protectiei Infrastructurilor Critice. http://ccpic.mai.gov.ro/directiva.html

[9] Avocanet.ro http://www.avocatnet.ro/content/articles/id_22140/OUG-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.html

[10] Monitorul Oficial: Strategia nationala privind protectia infrastructurilor critice (pdf) http://ccpic.mai.gov.ro/docs/HGR718_2011.pdf

This law defines a national critical infrastructure similar to definition offered previously in this paper but also introduces the term ‘European critical infrastructure’, defined as a national system or facility whose failure or perturbation would affect at least two EU member states.

At national level, the person directly in charge of all activities related to the identification, designation and protection of critical infrastructures in Romania is the Prime Minister, who in turn designates a state counselor on the topic. The national agency overseen by the PM and his or her state counselor is called the Coordination Centre for Protecting Critical Infrastructures (CCPIC), part of the larger Ministry of Internal Affairs (MAI). The CCPIC is the primary agency that ensures that all the activities implemented in accordance to European law (namely, directive 2008/114/CE) and the national law (namely, the OUG 98/2010 and its approval to law 18/2011) follow the purpose of developing and securing Romania’s critical infrastructures.

The agency is also an intermediary in communicating and maintaining partnerships with similar EU bodies, the European Commission itself, NATO, etc.

Within the law, CCPIC assumes several important roles. First, it connects public authorities and the owners, administrators or operators of the national critical infrastructures in order for them to carry annual evaluations concerning the status of the identified critical infrastructures, as well as submit similar evaluations to the European Commission once every two years. Public authorities are various ministries or public services institutions while the owners, administrators and operators can be, for example, private telecommunications providers or public energy providers. Second, together with homologues institutions in the EU and with the European Commission, CCPIC is involved in discussions for creating supplementary protection measures at EU level, based on each member state’s input.

The task of identifying critical infrastructures as such is itself complex. There is strict criteria in assessing whether an infrastructure should or should not be considered critical[11]. This involves, for example, calculating the number of people that would be harmed (physically) if that infrastructure would fail or be attacked, or the economical impact it would have (services/products being halted, loss of jobs), and finally to what degree would people mistrust the Government as a result of that failure or attack (because mistrust can directly affect the Government’s proper functionality). These various criteria are not cumulative, meaning that if an infrastructure ticks just one major impact from the criteria listed, it is considered critical. If it is the case, the CCPIC can alert the European Commission if it identifies a particular infrastructure outside the country (in another EU member state), that nevertheless could heavily impact Romania in case of failure or attacks. Then research, discussions and assessments will be carried by both countries and the European Commission and, if it is the case, the respective infrastructure will be named an European Critical Infrastructure. On the other hand, according to the law, Romania also has the duty to inform all other EU member states about its national critical infrastructures, particularly those that can affect them directly. If it is the case, a national critical infrastructure will become an European critical infrastructure following discussions and assessments from the EU member states involved.

All obligations stated in the law need to be respected by the various actors involved (public authorities, system administrators/operators/owners, other states etc). Heavy fines are stipulated by the law if otherwise.

[11] Idem 9.

2.2 Romania's national strategy on protecting critical infrastructure

What kind of security issues does the national strategy acknowledge in regards to national critical infrastructures? The terminology in this sense lists several important elements[12].

The first are vulnerabilities, defined as situations, processes and phenomena that either delay the critical infrastructure's capability to react to risks, threats and aggressions or in fact favours their emergence. Overlooking or bad management of a vulnerability can have serious consequences on the country's interests and objectives.

Risks are defined as particular contexts, elements or situations (internal and external) that favor the creation of a direct threat.

Threats are then considered capabilities, intentions, strategies and plans that aim to destabilize critical infrastructures by means of gestures, attitudes, or direct actions. The result of threats can include instability, insecurity and dangers of the critical infrastructures and the authorities and citizens relying on them.

Finally, aggressions are defined as attacks (military, cybernetic) that target the weakening or failure of critical infrastructures, with serious consequences for the everyday life.

All these types of security issues can refer to natural disasters, technical and technological errors, human errors but also intentional attacks such as military or cybernetic.

Based on these types of security issues, there are four major strategic objectives of the national strategy on critical infrastructures, as follow[13]:

1. To assure that there is a unitary approach on how they are identified, assessed and managed

2. To develop an early-warning system by integrating all existing networks and informational capabilities

3. To correctly evaluate all possible vulnerabilities and make sure they are addressed properly

4. To cooperate on the local, regional, national and international level on the topic of critical infrastructure security.

In order to reach these objectives, the actors involved must follow three main coordinates[14]: a) prevention, diminution and limitation of possible effects of critical infrastructure failure, b) accurate intervention should any type of crisis arise and finally, c) sustainability - developing means to create further support in risk analysis and crisis management.

In order for the objectives to be reached, the Government must invest in three types of resources[15]: legislative (creating and adapting viable legal frameworks in order to act efficiently and ethically), institutional (to rise the ability of public authorities in elaborating, implementing and monitoring activities that help reach the stated objectives) and most importantly human (trainings, public-private partnerships etc).

It is worth noting that Romania holds a strategic importance within NATO and the EU, particularly in the Black Sea area. However, while terrorism is a top priority in other member states, the level of alert on terrorism in Romania is kept at the 'cautious' level[16].

[12] Monitorul Oficial: Strategia nationala privind protectia infrastructurilor critice http://ccpic.mai.gov.ro/docs/HGR718_2011.pdf

[13] idem 12

[14] idem 12

[15] idem 12

[16] Serviciul Roman de Informatii http://www.sri.ro/sistemul-national-alerta-terorista.html

On the other hand, the country has been repeatedly stricken by natural disasters and hence the priority goes to protecting national critical infrastructures against these. Another top concern at national level is the technical maintenance and functioning of hardware and software used in many public institutions. Lack of proper modernization leads to gaps in the informatics system functioning, making them prone to cyber attacks or major technical failures. This explains why institutions such as the intelligence CyberInt body (part of the Romanian Information Services) has recently been created, particularly for the purpose of monitoring and assessing new challenges in the digital sphere of critical infrastructures and communicating them to relevant public authorities.

Conclusion

In conclusion, criticality resides in the ability of a system to rely on its vital infrastructures, but at the same time it is negatively defined as the quality of an entity, that if hindered, would cause system failure.

As the inter-connectivity of our globalized world continues to increase, critical infrastructure protection seeks to satisfy the sensitive balance between increased efficiency through virtualization on one hand and consolidated security on the other.

References:

[1] Alexandrescu Grigore. Vaduva Gheorghe. *Infrastructuri critice. Pericole, amenintari la adresa acestora. Sisteme de protectie*. Editura Universităţii Naţionale de Apărare „Carol I”. 2006. <http://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf>

[2] Avocanetnet.ro. <http://www.avocatnet.ro/content/articles/id_22140/OUG-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.html>

[3] Centrul de Coordonare a Protectiei Infrastructurilor Critice. <http://ccpic.mai.gov.ro/docs/HGR%201198_2012.pdf>

[4] Centrul de Coordonare a Protectiei Infrastructurilor Critice. <http://ccpic.mai.gov.ro/directiva.html>

[5] Monitorul Oficial: Strategia nationala privind protectia infrastructurilor critice (pdf) <http://ccpic.mai.gov.ro/docs/HGR718_2011.pdf>

[6] Serviciul Roman de Informatii. <http://www.sri.ro/sistemul-national-alerta-terorista.html>

[7] Serviciul Roman de Informatii. <http://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf>

[8] Steiner, Nicolae. Andriciuc, Radu. *Infrastructura critica. Vulnerabilitatile si protectia ei.* Bucuresti, 2010. ttp://www.academia.edu/4377219/Consid_priv_protectia_infrastructurii_critice>

[9] Uniunea Europeana htp://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm

[10] Wikipedia. ttp://en.wikipedia.org/wiki/List_of_stock_market_crashes_and_bear_markets