10.53477/2668-2028-21-46

SYSTEMIC APPROACH FOR CRITICAL INFRASTRUCTURES, HIDDEN VULNERABILITIES OF INTERDEPENDENCIES

Sorina-Denisa POTCOVARU, PhD Candidate
Lieutenant, Doctoral School, "Carol I" National Defense University
sorina.potcovaru@yahoo.com

Abstract: *The growing scientific interest in the field of critical infrastructure protection has been determined by society's growing dependence on the essential services provided by these infrastructures. Critical infrastructures do not work isolated, they establish complex and dynamic networks of interdependencies. A critical infrastructure is itself a system with its own components and operating principles, a system connected to a system of systems based on multiple determinations. Critical infrastructure systems are built based on interdependent relationships between infrastructures, manifesting itself as an open system that relates to the macro-social system. Critical infrastructure systems behave dynamically and react to external stimuli represented by threats. Interdependencies between critical infrastructures generate new vulnerabilities and threats, based on the spread of effects and consequences. A comprehensive approach for critical infrastructure risks requires a systemic approach, taking into account that the interconnection of critical infrastructure objectives also involves the interconnection of threats and vulnerabilities.*

Keywords*: critical infrastructure; system; interdependencies; threats; vulnerabilities.*

The critical infrastructures that provide a society's vital functions are not isolated and operate within a network of interdependencies. The critical infrastructure system is a complex one, in which several actors, state or non-state, are involved, some outside the government's control.

For their effective protection, critical infrastructures must be approached from a systemic point of view, in the form of systems of systems, taking into account the existing interdependencies at the sectoral and intersectoral level and the relationships with the environment.

The interdependencies and vulnerabilities of critical infrastructures

The critical infrastructure is a system, and its functioning is conditioned by the interactions between its components and subsystems: technic, security, safety, continuity. According to the literature, the critical infrastructure is composed of the following elements[1]:

- infrastructure nodes: installations, equipment, employees;
- the interactions between the infrastructure nodes: of administrative, decisional, operative nature;
- interdependencies with external entities: political, military, economic, social, technological, security.

This approach highlights the character of a dynamic and open system, with multiple internal interactions and with various relationships with the external environment.

Intersectoral criteria derive from the relationship of dependence between different types of infrastructure. These cross-cutting criteria are taken from Directive 114 of the European Union Council and transposed into national law. These are:

- the criterion regarding victims, evaluated according to the possible number of deaths or injuries;
- the criterion of economic effects, assessed according to the importance of economic losses or degradation of products or services, including the possible impact on the environment;
- the criterion on the population, assessed according to the impact on its confidence, physical suffering, or disruption of daily life, including the loss of essential services.

[1] Radu Andriciuc, *Considerații privind protecția infrastructurilor critice*, Editura Ministerului Afacerilor Interne, București, 2009, pp. 19-20.

The relationships between critical infrastructures result from the interdependence of vulnerabilities and associated risks. Thus, to have a comprehensive and realistic risk analysis, it is necessary to analyze critical infrastructures' systemic nature. In the literature, have been identified four categories of interdependencies[2]:

- physical;
- cyber;
- geographical;
- logical.

Two infrastructures are considered to be physically interdependent if each of their condition depends on the essential good or service provided by the other infrastructure. For example, a train transports coal to a power plant, and the power plant provides electricity for the railway warning system (light signals) or even for the locomotion of the means of transport, in the case of electrified railways.

Cyber interdependence assumes that the infrastructure state depends on the information transmitted through the information and communication technology infrastructures. This category of interdependencies emerged as a natural consequence of the rapid automation and computerization of infrastructures. The operation of critical infrastructures is increasingly dependent on computerized control systems. For example, SCADA (Supervisory Control and Data Acquisition) collects data from sensors and machines and transmits them to central management and control points. This interdependence causes the rapid spread of the effects of a cyberinfrastructure malfunction. In this context, the cyber risk is increasing as cybercrime uses new techniques and means and becomes a terrorist phenomenon.

On the other hand, cyberinfrastructures are affected by the dysfunction of energy infrastructures. Interdependence relationships generate cascading effects in a disruptive event and the propagation of the consequences that do not take into account borders. An instructive example is the North American power outage of August 14, 2003. The power outage in Ohio quickly caused adverse effects in several US states and even in Canada. It took only 10 seconds for the negative impact to spread and almost a week for the energy system to run at full capacity again.

Infrastructures are geographically interdependent if they are located in the same corridor. Thus, the effects of the malfunction of one infrastructure spread to another infrastructure due to geographical proximity. For example, an explosion caused by a terrorist attack on a power plant will affect other infrastructures within the blast range.

Critical infrastructures may be dependent in a way other than physical, cyber, or geographical, this being logical interdependence. Logical interdependencies are caused by cyber interdependencies as well as free-market relations regarding the purchase and sale of essential goods and services specific to critical infrastructures. For example, if the energy sector is affected by extreme natural phenomena or strained relations between the major economic powers, rising fuel prices will significantly affect the transport sector. The logical interdependence was also illustrated by the effects of bird flu on the health system and implicitly on the transport system. We can observe this kind of interdependence in the context of Covid-19 pandemics that affected all sectors of critical infrastructures.

[2] Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly. *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine 11, 0272-1708/01, December 2001.

According to another opinion in the literature, the relations between infrastructures are approached from 3 main perspectives[3]:

- How the functioning of one infrastructure depends on the other infrastructure systems, the interdependencies being established between the supporting infrastructure and the infrastructures that support it;
- Interdependencies can be approached of how other infrastructure systems depend on the services provided by the source infrastructure;
- The third perspective provides an overview of interdependencies' whole system in both directions between infrastructures.

The environment in which critical infrastructures operate is subject to permanent and rapid change and has significant influences on their protection needs. In a constantly changing society, where interdependencies at the critical infrastructures level are increasingly complex, vulnerabilities and threats must be analyzed according to the all-hazards approach theory. The interdependencies at the level of critical infrastructures and the development of the society reconfigured the risk management, replacing the threat-vulnerability approach with the view of the continuity of systems specific to the post-cold war period.

According to this approach, the risk to critical infrastructures is expressed as a function between vulnerabilities identified according to system continuity and threats identified after the all-hazards approach. For example, a container landing point at the intersection of shipping, road and rail is an intermodal terminal, which also connects to other infrastructures in the energy, industry and cyber sectors and which must be protected by applying systems continuity theory within the risk analysis.

Another aspect to consider in risk analysis is the escalation of adverse events from human, biological, meteorological, or cyber causes, such as terrorist attacks, extreme weather events - tsunamis, or cyber-attacks. The events of recent years and the growing interdependence between critical infrastructures require a rethinking of risk management.

The critical infrastructures system, an open and complex system

Moreover, between the critical infrastructures and the environment in which they operate, a series of economic, political, demographic, and social interdependencies are established.

A common method in specialized studies is modeling and simulation, used to identify and analyze the interdependencies between critical infrastructure elements. In the literature in the field, the interdependencies between critical infrastructures are analyzed in the context of an armed conflict, especially the fourth-generation conflict, where actions are not limited to the battlefield and the use of two opposing forces in violent kinetic actions. Thus, the literature proposed to analyze the interdependencies between infrastructures using modeling of effects-based operations (EBO)[4]. The authors propose integrating critical infrastructures in the Operation Net Assessment (ONS) process, the latter being an analytical process with a systemic approach of relationships, dependencies, vulnerabilities and strengths, based on PMESII factors: political, military, economic, social, information and infrastructure. The PMESII approach is relevant to illustrate the critical infrastructure system as an open system that is influenced and influences the environment in which it operates.

The systemic approach of the infrastructures in the form of systems that establishe connections with the environment described according to the PMESII factors is represented graphically in figure no. 1.

[3] Sara Bouchon, *The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual Stateof-the-Art*, Office for Official Publications of the European Communities, Luxembourg, 2006, p. 16.
[4] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, *Critical Infrastructure Interdependency Modeling: A survey of U.S. and international Research*, 2006, p. 22.

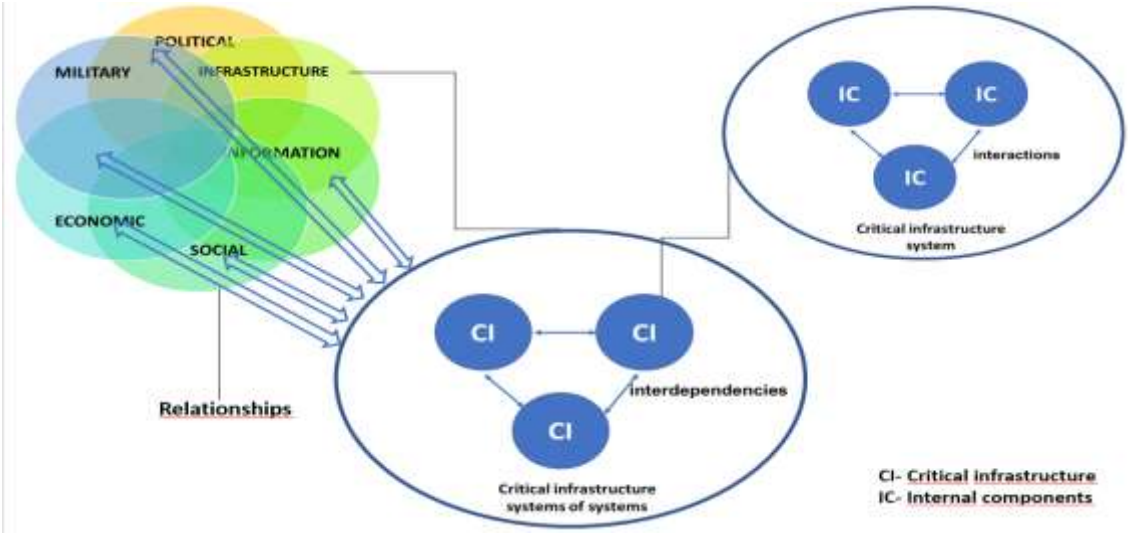

Figure 1: Systemic approach of critical infrastructure according to PMESII factors

One of the factors that influence the evolution of complex systems of critical infrastructures, determining their relations with the environment in which they operate, is represented by the actors involved, by stakeholders from the level of an infrastructure objective.

From the point of view of stakeholders, the following aspects are relevant

- public-private relationship and the degree of state control at the operator level:
  - public actor
  - private actor,
  - mixed actor (with different degrees of state involvement, most often as a shareholder, or in some form of public-private partnership).

From the point of view of the analysis on public-private levels, the degree of regulation and standardization of the infrastructure activity at the national and international level is also relevant, as well as the existence of specialized authorities or bodies of law, supervision, or control. For example, there are such bodies as the National Energy Regulatory Authority and the National Commission for Nuclear Activities Control at the Energetic sector level. Also, in connection with the public-private relationship, the operator's purpose is essential, distinguishing between making a profit and providing public services:

- form of organization (companies, associations, multinational companies);
- form of financing and economic situation;
- national-international relationship.

First, we must consider the national or international character of the holders, administrators, or operators of the objective and the degree of involvement of the national element. The international aspects increase the complexity of protection activity, taking into account the interest of states and international organizations for vital resources and strong determinations in international relations at a political, diplomatic, military, and economic level.

The internationality of critical infrastructure must be analyzed from several points of view:

- nationality of actors and stakeholders;
- territoriality – the location of the infrastructure, as well as the location of the infrastructures with which it interacts;
- propagating the effects and consequences of a malfunction or destruction of infrastructure beyond the borders of a state;
- localization of the supply chain with raw materials and services necessary for the operation of an infrastructure;

- localization of the distribution network of essential services and goods to the beneficiaries.

The system of critical infrastructures can be described by the relationships established between stakeholders, such as control, subordination, regulation, ownership, administration, and supply.

From the point of view of the flow of vital resources along with the interdependencies, the following are relevant:

- the network of key suppliers;

The issues related to the security of the supply chain and the degree of infrastructure self-sufficiency in vital resources flow are important. The degree of autonomy can be analyzed both at the level of infrastructure and the national level, referring to the dependence on other operators or other states for raw materials and services essential for the continuity of safe operation.

- the network of beneficiaries

From the beneficiaries' point of view, vulnerable groups of the population and other critical or special infrastructure consuming essential goods or services are relevant. The supply chain of essential good and services provided by critical infrastructures is represented in figure no.2:

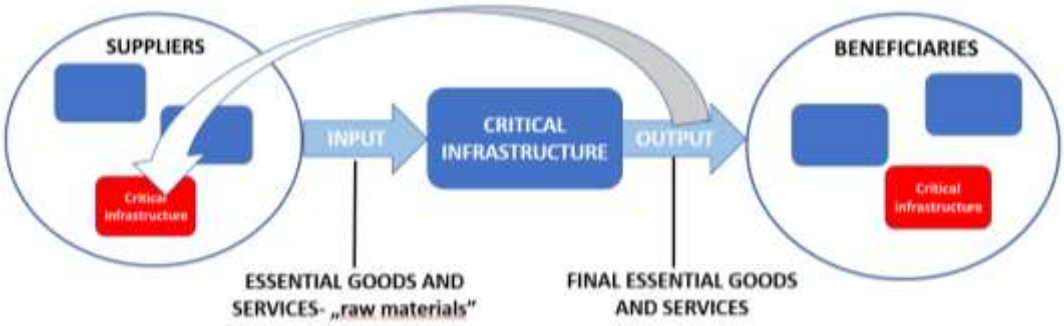

Figure 2: The supply chain of essential goods and services- a physical interdependence

Interdependencies appear when the provider and the beneficiary are the same critical infrastructure, and the vulnerability of such a node is even greater.

Conclusion

Multiple interdependencies are established between the critical infrastructure sectors, forming a complex system. Infrastructures cannot operate in isolation and a systemic approach leads to more efficient and comprehensive risk analysis. Also, the interdependencies network depends on the state of the infrastructure - the state of regular operation, dysfunction, and following a disruption.

There are systems, agents in interaction at the level of infrastructures, and internal processes that aim to fulfill vital functions, respectively the provision of essential products or services characterized by nature, quantity, and quality.

The complexity of the interdependencies at the level of critical infrastructures presents the disadvantage of the rapid propagation of the effects of a disruptive event and the possibility of removing these effects from the level of one infrastructure by using the facilities of another infrastructure. In this context, the protection of critical infrastructures must consider complex plans, organizational responses, interinstitutional and international cooperation, with close and objective supervision by mass media.

BIBLIOGRAPHY

1. ANDRICIUC Radu, *Considerații privind protecția infrastructurilor critice*, Editura Ministerului Afacerilor Interne, București, 2009.
2. BOUCHON Sara, *The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual Stateof-the-Art*, Office for Official Publications of the European Communities, Luxembourg, 2006.
3. PEDERSON P., Dudenhoeffer D., Hartley S., Permann M., *Critical Infrastructure Interdependency Modeling: A survey of U.S. and international Research*, 2006.
4. RINALDI M. Steven, Peerenboom James P., and Kelly Terrence K. *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine 11, 0272-1708/01, December 2001.
5. ***, *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 Unio, L345/75.