sciendo

Land Forces Academy Review
Vol. XXIII, No 4(92), 2018

IMPROVING THE LEVEL OF CRITICAL INFRASTRUCTURE PROTECTION BY DEVELOPING RESILIENCE

Ionuţ Alin CÎRDEI
"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
cirdei_alin@yahoo.com

ABSTRACT

Modern society is characterized by the increasing interdependence between the actors of the international environment, in the conditions of globalization of all the fields of social life. Increasing interdependencies, together with the emergence of new risks and threats, which attempt to exploit systemic vulnerabilities, which are increasingly numerous and difficult to eliminate, bring a new issue to states and other security environment actors: to ensure the protection the infrastructure elements that are indispensable to the normal activity of the population, economic agents, non-governmental organizations and state institutions. Critical Infrastructure Protection becomes an important point on the agenda of all decision-makers who are in a position to counter the asymmetric threats that jeopardize national interests and democratic values. Due to the multiplication of risks and threats and the multiplication of interdependencies between the various infrastructure elements, the protection of critical infrastructures can not be achieved effectively only by ensuring their physical protection. The cascading effects of a disturbance can be felt at the level of society as a whole, and it is therefore necessary to address the issue of ensuring the protection of critical infrastructures in a comprehensive manner including infrastructure and community resilience issues.

KEYWORDS: infrastructure, protection, resilience, complementarity

1. Introduction

The elements of infrastructure have emerged from the need to meet people's needs and have evolved over time in line with the pace of development of human society. The oldest method of the human being to gain individual protection was the accession to human groups, tribes, communities, states or other forms of organization to ensure the absence of risks and threats of any kind (Bojor & Motofelea, 2011).

The first elements of the infrastructure used by man responded to basic needs and consisted of housing elements and simple and unconsolidated roads. Subsequently as knowledge evolved, as technical development of human society has increased, we are also witnessing a multiplication and diversification of infrastructure elements. For example, in ancient Rome, we encounter upgraded communication paths and other public utilities such as squares, temples, public baths, arenas, aqueducts, etc. Also, taking into account the development of technologies and the widening of the human horizon, including increasing the limits of the known world and increasing the distances and the volume of goods transported, we are also witnessing a diversification of the environments where these elements of infrastructure exist. The development of trade has led to the emergence of ports, shipbuilding sites, and

DOI: 10.2478/raft-2018-0028

so a new dimension has been conquered. In the time, to the two classical dimensions (terrestrial and naval), the air, cosmic and informational dimension has been added, which has led to the development and multiplication of infrastructures, as well as to multiplication and diversification of threats, also fueled by the increased vulnerabilities of the new systems. With the increasing dependence of society on infrastructure elements, they have become critical, meaning that the impact that an infrastructure element can have is quite important. The level of criticality of an infrastructure depends on a number of factors, such as: the number of victims of an possible incident, the economic and social impact of service unavailability, the reconstruction or restoration period of the infrastructure, local, regional or international effects of the unavailability, the infrastructure uniqueness and so on. In view of these considerations, we can define critical infrastructures as elements, systems or system components which are essential for maintaining the vital functions of society, health, safety, security, social or economic well-being of individuals and whose disruption or destruction would have a significant impact at regional or national level due to the inability to maintain those functions (OUG 98, 2010).

Nowadays, the infrastructure elements are no longer isolated. They are linked by different systems of other infrastructure elements, and the mode of operation of an element can influence directly or indirectly the functioning of another, these being characterized by a state of interaction. Also, the influence that a critical infrastructure can have on the external environment is not only about the elements that are directly related to it, but it is felt through a complex mechanism at the level of the whole society, which gives rise to new vulnerabilities and obliges to take additional protective measures. However, total protection is not possible and the multitude of risks and threats from all environments and with varied and unpredictable manifestations make it impossible to anticipate all the effects and to adopt appropriate physical protection measures. In order to increase the level of protection and to protect the infrastructures and society from the effects of disability, a comprehensive approach to critical infrastructure protection is needed, including resilience issues, seen as a possible short- and medium-term solution to accidental or intentional disruptions at the level of critical infrastructure.

2. From the Protection of Critical Infrastructure to Critical Infrastructure Resilience

Providing total protection at a critical infrastructure level is not possible for both financial considerations and due to threats and vulnerabilities that are constantly evolving and transforming, so that processes, systems or individuals can cause accidents or incidents and intentional acts or attacks may occur. Whatever safeguard measures would be implemented at some point, sooner or later they could crumble. That is why all entities involved in the provision of infrastructure protection are aware that the effective protection of infrastructures needs to be complemented by the development of resilience.

Although the protection and resilience of critical infrastructures are complementary to a complex risk management strategy, we must accept the differences between them. Thus, protection refers to the ability to prevent or reduce the effects of an unpleasant event, while resilience consists in the ability to reduce the magnitude, impact, and duration of an interruption in operation, and contemplates a snapping approach to all components and processes, from physical components, to management capacity and human resource quality, to develop and maintain the ability to prevent, absorb, adapt and recover after an attack of any kind.

Resilience is a concept that has its origins in the field of psychology and refers to the ability of the human body to adapt as a result of a change in the general situation due to traumas, tragedies, threats or other stress-causing events. Resilience is manifested in most situations, but its level varies with person, being more of an acquired but innate trait, meaning that it can be learned and developed at all times. The concept of resilience, due to its versatility, has also been adopted in the field of security, where it is understood as a mix of factors contributing to the strengthening of security through indirect measures and actions. In the field of critical infrastructure protection, resilience should be seen as a way to increase their security by identifying measures that can be taken both at critical infrastructure level, but especially at the level of organizations and processes that provide inputs or use the outputs of that infrastructure. Critical infrastructure resilience implies integrating all factors within an organization or system into an internal and external environment as well as identifying and understanding all the interdependencies between different elements and especially the effects that different events or incidents may have on the population, the infrastructure elements and the processes between them.

Resilience can be defined as, "*the ability of an infrastructure to prepare to cope with changing conditions and adapt to them, and to resist and recover rapidly from disruption, including deliberate attacks, accidents or natural events*" (Presidential Policy Directive, 2013). In this respect, the infrastructure elements need to be robust, agile and adaptable, so that all the activities carried out can contribute to the strengthening of their resilience.

Resilience can be addressed from the perspective of its four basic dimensions (Bruneau et al., 2003):

- Technical resilience refers to the ability of an organization to cope with a widespread crisis and to maintain its systems functional;
- Economic resilience takes into account the capacity of critical infrastructure to cope economically and financially with all the challenges that arise from the crisis;
- Organizational resilience is centered on the organization's decision-making system and its ability to adopt coherent measures tailored to the concrete situation, aimed at overcoming the crisis and mitigating its consequences;
- Social resilience refers to the ability of society to absorb and reduce the impact of an unforeseen situation that impacts both critical infrastructure and society as a whole.

According to studies and specialized analyzes, the main characteristics of the infrastructure elements underpinning the development of resilience are (National Infrastructure Advisory Council, 2010, p. 16):

- *Robustness,* understood as the ability to continue operating even under the circumstances of a serious accident or incident. Robustness can mean the constructive resilience of critical infrastructure or its modularity, and the ability of various constructive elements to overtake certain processes into critical situations, and can be reinforced by a series of measures such as: preparing to cope with a crisis situation, system redundancy, the ability to detect harmful events, the ability to react and the intrinsic physical strength of the system;
- *Resources available.* In order to withstand to the changing environmental conditions, a critical infrastructure must have the resources needed to manage a disaster as it unfolds. This includes identifying options, prioritizing what needs to be done both to control the damage and to start mitigating them and communicating the decisions of the people who will implement them. An extremely valuable resource that can put the value and efficiency of using other resources is represented by the human resource that needs to be prepared to manage any kind of crisis situation;

- *Rapid recovery* consists of the ability to restore the entire system or its essential parts within a short time after a disaster or incident. The recovery capacity can be amplified by the existence of realistic action plans and verified through exercises and simulations, the existence of emergency systems, as well as the necessary means and resources. Recovery capacity can be determined by the existence and availability of material resources, the availability of financial resources, the availability of human resources prepared to act, and the existence of processes that facilitate rapid recovery;
- *Adaptability* centers on the idea of learning from mistakes and past experiences. It may consist of reviewing plans, modifying procedures, introducing new technologies as a result of a crisis, to increase robustness, recovery capacity and resources before the onset of the next crisis.

In the field of critical infrastructure protection, operators and their owners have an extremely important role to play, as they have to cope with an environment characterized by the continuous evolution of threats and vulnerabilities, and must therefore identify dynamic and tailored solutions. In addition to the specific measures aimed at ensuring the protection of critical infrastructure, resilience aims at putting into operation all possible mechanisms and measures, physically and logically, along with mechanisms that provide redundancy and error tolerance, capable of adapting the system to the volatile environment, reduce its reaction time and increase remodeling capacity (Bologna & Carducci, 2016).

The resilience of a system is very difficult to measure and build, and it can not be at the same level for any threat or disruptive event. Resilience must be built in a unique, tailored way, taking into account possible security challenges, since each disruptive event affects the system differently and therefore requires adapted measures to return to normal and the consequences to be minimized.

A resilient system is a system capable of anticipating disruptive events, regardless of the form, intensity, environment, and way of manifestation, to absorb the impact of unexpected events and to reduce their consequences and to allow the system repair and restoration. Resilience is difficult to build and measure, the best way of measuring resilience beeing during and after real events. However, in order to develop resilience, measures can be taken long before the potentially destructive events occur, and a good way to identify the risks, threats, vulnerabilities, interconnections and interdependencies, as well as to identify the measures that can be taken in the strengthening of the whole system and the system of systems in which the infrastructure element is included is the continuous development of an analysis and evaluations. In this respect, the risk management process, which must be a continuous, realistic process that allows identification and testing of solutions and their implementation, has a particularly important role to play. Risk management needs to be complemented by complex analyzes that highlight all the interdependencies between the infrastructure element and other critical infrastructures, both at the entry and exit levels, as well as the connections and influences that can occur both in the operation area and in the extended area, involving not only the institutions and organizations, but also the civilian population, which is most exposed to the direct and indirect consequences of disturbances and accidents or attacks. Security and resilience are strengthened through the risk management process, which can be seen as a complex, ongoing process aimed at identifying and analyzing risks, and adopting optimal measures to neutralize or reduce it to an acceptable level from the perspective of consequences or costs.

In an effort to ensure the security of a critical infrastructure, protection measures and those aimed at increasing resilience are

complementary and intertwined, so it is very difficult to have a separate approach. A secure, resilient critical infrastructure operating at optimal parameters requires effective information exchange between authorities at all levels of decision-making and infrastructure owners as well as between owners of different infrastructure elements in order to facilitate the timely dissemination of information related risks and threats, as well as information that allows action synchronization and effort concentration during incidents. The exchange of information implies the existence of common procedures, a secure, interoperable, redundant communication infrastructure (Presidential Policy Directive, 2013), which will work even if the classical communication system are shut down.

A resilient system is a system capable of anticipating and absorbing potential disturbances, developing adaptive means, and setting responses directed either to create the ability to withstand disruption or to recover as soon as possible after an incident (Royce & Behailu, 2014), but in order for these things to materialize, it is also necessary to develop a specific culture that promotes resilience and maintains in contact all entities that can play a role in the process of protecting critical infrastructures and that may be affected by the consequences of unforeseen events or which may contribute directly or indirectly to restoring normal functioning and limiting the consequences. The whole system must work in an efficient manner, and resilience needs to be addressed long before a crisis arises because resilience develops rather hard, with human and material effort, and failing that it is possible that remedial attempts to amplify the negative effects of potential natural or man-made disasters (Fisher & Gamper, 2017). From this perspective, resilience must be seen as a supplementary layer of protection, which strengthens not only the security of the infrastructure element but also of the entire society.

Developing resilience is very difficult to accomplish and, as mentioned above, involves multiple efforts by all actors with responsibilities in the field. Although the effectiveness of measures aimed at increasing resilience is difficult to quantify, and for different infrastructures and hypothetical situations different measures and approaches are needed, resilience plays a role as a multiplier of security and needs to be addressed with the utmost seriousness.

Resilient systems, especially in the areas that meet the basic needs of society, are built in a way that allows them to operate under extremely difficult conditions, they allow anticipation of destructive phenomena, shock absorption and rapid adaptation to new conditions by spreading shock wave and redirecting efforts, which allows for the quickest recovery and damage to as few people as possible. An area in which the development of resilience, in the complementarity of protection measures, has allowed us to achieve good results is the energy one, where we can see that the national and international electricity supply systems are extremely well designed, have a modular construction, are complementary in most cases and allow intervention in almost any condition, with the least possible harm to consumers. This is evidence that the development of resilience can play an important role in enhancing the security of the infrastructure elements and, more specifically, in creating the conditions for them to fulfill their basic role of ensuring the availability of essential goods and services for proper functioning of society and for its safety.

3. Conclusions

Critical infrastructure resilience can be seen as a quality that reduces vulnerability, minimizes the consequences of a threat, accelerates response and system recovery, and facilitates adaptation to a destructive event (Rehak, Senovsky & Slivkova, 2018).

Developing resilience complements measures to achieve critical infrastructure protection, which is more relevant to their physical protection, and must be seen as a component of a more complex system that targets a much wider area and more actors, each with the own features and with own vulnerabilities and strong points.

In the context of critical infrastructure protection, resilience is only one component, a wheel of an extremely complex mechanism, which must be based in its functioning on the implementation of the concept of defense in depth, which means the existence of more layers, more defensive levels, in which each element contributes to securing the ensemble by performing basic functions and taking into account the cascading effects of different incidents. Resilience plays an important role in achieving critical infrastructure security and requires for its implementation a change in approach regarding the need to achieve critical infrastructure protection, from a local approach that takes into account the immediate, direct consequences, to a comprehensive approach, including all actors involved or affected, and the entire network of connections and dependencies. Resilience can be built based not strictly on the need to ensure security, but on the effects-based approach. To increase resilience, a comprehensive, multidimensional approach to critical infrastructure security is needed. It would also be useful to develop modular infrastructures, subdivided into subsystems that can be separately secured as part of the whole and which can be more easily managed in the perspective of an unforeseen event with negative consequences.

Developing resilience in order to increase the security of critical infrastructure is of particular importance as it can strengthen the economic dimension by ensuring the continuity of different businesses, increase the preparedness of communities to deal with disruptive events, contribute to the exchange of information between infrastructure owners and institutions with responsibilities in the field of emergency interventions, increases the efficiency of the state institutions with attributions in the field and makes the whole society and the state safer.

Ensuring the protection of critical infrastructure is a shared responsibility between infrastructure owners and the state. Infrastructure owners need to take optimal risk-based protection measures and the state through its institutions must create the appropriate legislative framework and directly and indirectly support infrastructure owners in their efforts to protect and mitigate their consequences unpleasant events. Resilience in the field of critical infrastructure is more than that, being a shared responsibility between the private sector, the government, the community and individuals, as each has its own role in creating and developing resilience, implementing specific measures and recovering as quickly as possible after incidents. Resilience implies a comprehensive approach to the entire system that includes critical infrastructure, upstream and downstream organizations as well as all structures, entities that can be directly and indirectly affected by interdependencies and connections.

REFERENCES

Bojor, L., & Motofelea, G. (2011). Aspects of local communities security in hybrid warfare, *Revista Academiei Forţelor Terestre no. 3 (63)*, 243.

Bologna, S., & Carducci, G. (coordinators). (2016). *Guidelines for Critical Infrastructures Resilience Evaluation*, available at: http://www.infrastrutturecritiche.it/new/2016/04/25/linee-guida-valutazione-resilienza-delle-infrastrutture-critiche-gruppo-di-lavoro-2/.

Bruneau, M. et al. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities, *Earthquake Spectra, 19,* 733-752, available at: http://earthquakespectra.org/toc/eqsa/19/4.

Fisher, M. K., & Gamper, C. (2017). *Policy Evaluation Framework on the Governance of Critical Infrastructure Resilience in Latin America*, p. 8, available at: https://publications.iadb.org/.

National Infrastructure Advisory Council. (2010). *A Framework for Establishing Critical Infrastructure Resilience Goals, Final Report and Recommendations by the Council*, available at: www.dhs.gov/publication/niac-framework-establishing-resilience-goals-final-report.

Ordonanţa de urgenţă nr. 98 din 3 noiembrie 2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, available at: ccpic.mai.gov.ro/docs/OUG_98.doc.

Presidential Policy Directive – PPD21. (2013). *Critical Infrastructure Security and Resilience,* available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Rehak, D., Senovsky, P., & Slivkova, S. (2018). *Resilience of Critical Infrastructure Elements and Its Main Factors*, *Systems*, *6*(2), 21, available at: https://www.mdpi.com/2079-8954/6/2/21.

Royce, F., & Behailu, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems, *Reliability Engineering and System Safety*, *vol. 121*, 91-92. available at: https://www.sciencedirect.com/journal/reliability-engineering-and-system-safety/vol/121/suppl/C.