CRISIS MANAGEMENT OF CRITICAL INFRASTRUCTURES

Vice-Admiral (ret) Professor Engineer Ion Alexandru PLAVICIOSU, PhD*
Anna STRONS**

The present paper presents that it is useful to modernize the actual system by creating a governmental organization, unique and permanent, whose purpose is to elaborate the intervention and protection actions in crisis situations, and which is capable to control the means and resources at both the national and local level in order manage them efficiently. In the case of critical infrastructures whose management is made by information systems, the protection and intervention role must be undertaken by the system administrator who has to permanently analyze the threats and activate protection measures.

Keywords: *crisis management; critical infrastructures; errors in the system's configuration; the protection of critical infrastructures; the national interest*

Critical infrastructures can be defined as complex systems with physical and/or virtual structure designated to manage the function, use, and maintenance of important activities and processes at national, regional, and even global levels, whose total or partial collapse or alteration of essential parameters leads to major negative influences on the population or economic area in which they function.

According to other definitions[1], critical infrastructures are those infrastructures with an important role in securing the continuous operation of systems and performance of economic, political, information, and military processes.

The crisis of a critical infrastructure can be determined by errors in the system's configuration when not all elements related to the system's operation were considered, or unrealistic or non-conforming weight was allocated to these elements, by hostile forces

* Vice-Admiral (ret) Professor Engineer, PhD, Member of The Academy of Romanian Scientists; e-mail: alexplavion@yahoo.com
** anca_plavi@hotmail.com

1 Grigore, Alexandrescu, *Critical infrastructures. Dangers and threats to these. Protection systems.* NDU Publishing House, 2006.

aiming to destabilize the system, or by natural and environmental causes. A critical infrastructure at the national level is a system or a component of a system, found within the national territory, which is essential for maintaining the vital functions of the state and society, health, security, social and economic welfare of the population and whose disturbance or destruction would have a significant impact at the national level because of the inability to maintain the said functions[2]. The protection of critical infrastructures in our country, according to the documents issued by the government, is designed to secure their functionality, continuity, and integrity, and to prevent, eliminate, neutralize a threat, risk, or weak point. The protection of critical infrastructures includes the ongoing activity regarding the risk analysis and evaluation, the security of classified information protection, accomplishment of security plans for critical infrastructure operations, fixing the control points and manner of communication, as well as maneuvers, reports, reevaluations, and updates of the elaborated documents.

The approach towards the problems of critical infrastructures' crises is made differently depending on the natural or anthropic character of the causes that generated their occurrence. The fact should be emphasized that solving crises in democratic regimes must be made based on carefully studied scenarios which are planned ahead of time based on risk and vulnerability analyses to prevent the local administration, which can be of a different political color than the government, to direct the population support actions to the needs for political capital.

Another aspect of critical infrastructure crisis problems might be their multiplication and diversification at national and international level subsequent to technical and technological development. In this context we can discuss a certain "mobility" of the critical infrastructures correlated with technical and technological evolution, which includes or excludes systems, depending on their importance within the national economy. This is the reason why keeping critical infrastructures under control is a permanent task of the authority accredited at the national level to control this problem.

Nowadays, the critical infrastructures have a high level of diversity that include information systems from various fields of national interest (e.g. health, banking, population census, border police, agricultural and urban cadastre, etc.), government activity, energy infrastructures (electric energy and fuels), transportation infrastructures, information systems for controlling industrial processes, especially within industries with high potential for chemical or radioactive pollution. The importance of each system of the national economy, and implicitly the effects of the crises within the systems will depend on the level of economic development of the country.

[2] Government Emergency Ordinance No. 98/2010, on the identification, designation and protection of critical infrastructures.

The destabilizing factors with the highest impact over critical infrastructures, and also the hardest to predict the magnitude of the damage they cause, are the natural ones: earthquake, land slide, flood, and dam breakage. This is the reason why the areas that might be affected by these disasters must be identified ahead of time. The consequences must be evaluated, and plans must be drawn up to evacuate the goods and the population, to hospitalize the wounded, to clear the affected areas, and to restore the production capacities. Natural disasters especially affect transportation infrastructures, electric energy providers, communication systems with ground equipment, civilian and industrial buildings, and households. For a more accurate and realistic evaluation of the damage caused by a natural disaster and in order to decrease the mitigation effort, and to assist the population in the disaster area, it is mandatory to take some steps before it occurs: to create a data-voice communication system via satellites independent from any ground infrastructure. These systems already exist and are operational with global coverage, i.e., IRIDIUM and THURAYA. Besides data-voice communication, both systems have a GPS module incorporated in the phone which enables its precise location. The connection between users is made directly via the satellite without the necessity of using any technical ground infrastructure. This allows the latter to be utilized solely to call land line phones; to equip the rescue team with audio and video communication systems independent from the ground infrastructure. When a disaster or a catastrophe has occurred, the intervention and rescue teams' members must be able to freely and easily communicate between each other and with the command center. During the recent catastrophes in Chile and Haiti caused by earthquakes, or in Pakistan by floods, or in other numerous instances, all ground communication channels ceased to function; putting them back in operation was a crucial task for the rescue teams and endangered the population. Portable equipment with GSM and GPS incorporated, operated by one operator, with an independent energy source, which can be installed and operated at short notice, and therefore ideal for supporting the rescue teams' operations has been created for these types of situations; to equip the mobile intervention units with a "fleet management" type of route management system based on GPS tracking of each vehicle with digitized maps, and communication of the data to the command center via satellite telephony. In this way, the use of intervention units, relocation or change of routes depending on the needs is optimized.

Satellite images of the disaster areas are extremely useful when floods occur (and not only floods) in order to assess the size and extent of the disaster, to establish the means to clear the flooded area by controlled flooding of the adjacent areas, overflowing the artificial lakes, and utilizing the regulatory effect of dams. The technical means described above facilitate specialized intervention in areas of highest need, surveillance of the way the population and economic objectives are assisted, the necessary steps in order to contain and mitigate the effects of the disaster, and restore social and economic activities.

In Romania there are floods every year, usually in the same very well-known and precisely delimited areas, which produce damage of hundreds of millions lei.

The accomplishment of an early warning system and an infrastructure for assisting the intervention and damage reduction would cost a small percentage of the amounts spent to provide disaster relief. The central administration would rather help the victims to rebuild their houses, sometimes on the same sites, than allocate funds for infrastructure works meant to protect the easily flooded areas. Based on the social solidarity concept, they introduced a mandatory insurance against earthquakes and floods which has to be paid by all household owners even when they live in areas with no floods or earthquakes. The insurance companies might financially support programs for the accomplishment of protection systems in easily flooded areas taking into consideration the fact that they can maximize their profits by reducing the amounts paid as damages. The government can also take firmer steps by forbidding construction in these areas.

Communities from potential natural risk areas must take the steps resulting from the risk and vulnerability analyses in order to diminish damage as much as possible. Past experience shows that these phenomena are lightly regarded, and the problems arising in the aftermath of natural calamities are very often ignored and do not constitute a starting point for future protective actions. In January and February 2010 there were two powerful earthquakes in Haiti and Chile[3], respectively. The earthquake in Haiti had a magnitude of 7.0 and affected approximately 3 million people, killed 310,000, injured over 300,000 and massively destroyed the infrastructure, businesses, ports, and homes. By comparison, in Chile 562 people died and the material damage was much smaller despite the fact that the earthquake's magnitude was over 8.0. This is the result of the application of strict and drastic rules regarding civil engineering projects, and also of the severe punishments for those who violate them. Also, it adds to the above mentioned fact that the plans to assist the population and businesses in case of a disaster are very well developed and practiced. These things make a difference, and they can drastically limit, in case they are applied, the consequences of any natural disaster. The problem seems to be simple, but it is difficult to execute it in a frail democracy when the politicians are more interested in their political group's interests than in the major interests of the population.

In December 2004, there was a powerful seismic event in the Indian Ocean with the epicenter lying west of the Indonesian coasts and Sumatra Island. The seism produced a devastating tsunami wave that crashed on the shores of 11 abutter states, with wave heights over 30 meters causing over 230,000 deaths and huge material damage which could never be exactly quantified. This was one of the biggest natural disasters ever recorded and it mainly affected Indonesia, Sri Lanka, India, and Thailand. The states and the populations affected by it

[3] The 26 December Tsunami; Journal La Houille Blanche no. 2/2995.

received prompt aid from the international community worth over 14 billion, but the situation in that area is still far from what it used to be before the disaster.

Considering that it is a well known fact that the Indian Ocean has a high seismic potential, the normal question that arises here is why they did not realize ahead of time and, at a substantially smaller cost than the damage which occurred, install early warning systems which could have saved a considerable number of human lives and economic objectives. The speed of the waves caused by the earthquake in the offing was between 500 and 1,000 km/h, and at the shores the speed decreased to the order of tens of km/hr. The conclusion is that there was enough time after the earthquake had occurred to warn the population to evacuate from the exposed areas.

By comparison, the March 2011earthquake, which had the epicenter at approximately 130 km east of the coast of Japan, at a depth of 32 km and with a magnitude of 8.9 on the Richter scale, created a tsunami whose waves were over 40 meters high in the ocean and which hit the shore by 10-meter waves, causing huge destruction of infrastructures on a distance of 10 km, including the destruction of the Fukushima nuclear plant, and about 20,000 deaths[4]. The damage was diminished due to the early warning system which functioned and alerted Tokyo one minute before the effects of the earthquake were to be felt there. The plans and programs to mitigate the effects of the disaster were applied after its occurrence. In this way, Japan rapidly recovered its potential by the involvement of the entire population of the country, despite the fact that it had gone through a powerful economic crisis in the context of the world crisis.

Critical infrastructures might be exposed to the concerted destabilizing actions of persons, terrorist groups, or hostile institutions which gave up the classical means of the "cold or hot war," and are trying to destabilize the state economies of the countries considered an enemy, causing major crises that have important economic implications.

Some political analysts assert, based on pertinent reasons, that "the code wars are more efficient for destroying the economic potential of the enemy than other types of war."

After the "cold war" the war against terrorism followed, also called asymmetric threats, and nowadays we are facing the "code war" as stated by the former CIA agent Cofer Black at the Las Vegas Information Exhibition in July 2011. According to a report elaborated by McAfee Company, more than 70 governments and organizations, including UNO agents and American military industry organizations have been the targets of cyber espionage attacks. Analysts assume that the attacks originated from China, but they do not exclude the penetration of Al Qaeda and other terrorist organizations in the cyberspace.

[4] Damage Situation and Police Countermeasures Associated with Tohoka District – off the Pacific Ocean Earthquake – Japanese National Police Agency, 20.04.2011.

An operation began in 2006 by intrusion into the servers of a South Korean construction company and continued until 2011; the authors of the attack were mainly interested in data regarding the American defense and satellite communication systems.

The unauthorized access to information systems sets the conditions to deploy virus attacks against them, destroy the information, and deteriorate the management. When the target is a critical infrastructure management system, the disruption of their functioning, even partial, might have major negative effects for the economy and population.

In July 2010, experts from Germany discovered the virus called Stuxnet which was created to affect the SCADA data acquisition system belonging to Siemens, which is mainly used to manage the water supply, oil platform activity, power plants, and industrial installations. Many attacks were reported in Iran, Indonesia, India, and the US.

The virus appeared initially in Iran where it attacked over 30,000 computers integrated in the command system of industrial processes and the Iranian nuclear program, and caused great concern among the experts in information security. The target of the attack and the region in which it appeared suggest it was created by a group of professional hackers, and its main purpose was not the espionage of the affected systems but the initiation of sabotage actions. According to Kasperski Lab, the virus can attack computers which are not connected to the Internet, by simply connecting an infected USB to the central unit. This shows that the creation of the virus was supported by the officials of a state which holds important and valuable information. The specialists' opinion is that Stuxnet is the prototype of a cyber weapon which will lead to the creation of new and very dangerous attack instruments, and that this time the world faces a cyber arms race and a new era of cyber terrorism.

The states are interdependent and sometimes complementary because of economic globalization, thus the crises of critical infrastructures are transboundary. This is the reason why the complexity and interdependence of critical infrastructures implies the development of procedures and technologies correlated at national and international levels, in order to identify the threats and to protect against them. It is easy to understand that a malfunction of the information, cybernetic, industrial, energy, and transportation systems is of a nature to cause a cascading propagation of the destructive consequences.

It is practically impossible to ensure the protection of all critical infrastructures or 100% protection for any of them. That is why the prevention and protection elements must be implemented by responsible factors at the national level, the priority being those services and facilities whose interruption or malfunction cause destabilizing effects to the national security, economy, population health, or assurance of basic vital necessities, i.e., energy, water, food, trade and banking services.

Specialists have extensively analyzed the problems of critical infrastructure crisis management, physical and virtual, and have set up methodologies for approaching the relevant aspect related to vulnerability analyses; risk factors and their importance; means to discourage, prevent, and protect against the threats; interdependencies between critical systems at national and international levels; and elimination of the negative consequences

of a crisis. One of the main problems of the risk management of critical infrastructures is the organization of planned actions for this purpose and determining the organizational structure of the institution accredited to perform this activity.

The organization prepares the realization of the planned actions by allocating the necessary human, material, and financial resources. The organization implies the concrete and early definition of the planned actions which turn into tasks, the classification of the activities in a function which can be given to a person or institution which become responsibilities, the conferment of competencies and authority to each function (position), and the indication of necessary qualification and level of training in order for each function to be accomplished to its best. Taking into consideration the mobility of critical infrastructures, their continuous evolution given by the development of the technologies and social organization, diversification and amplification of threats, various solutions have been proposed for crisis management.

It is worth favoring the version of creating a governmental institution with permanent activity in this field empowered to solve the problems related to the multitude of specific aspects which characterize the management of critical infrastructures crisis. This institution should be prepared to act especially in crises situations caused by natural phenomena and environmental accidents. To give just one example, the US has created a governmental institution, National Infrastructure Protection Plan (NIPP), which represents the integrated frame for risk management, in which there are clearly defined roles of critical infrastructure protection and the responsibilities of all governmental institutions, private and non-governmental organizations, and other institutional or social partners[5]. They defined the key areas from the point of view of infrastructures and resources which necessitate protection measures against risks. The plan was submitted for a public debate, after which the national institution named the Department of Homeland Security was created for centralizing objectives and resource management and for operational decentralizing by defining the components and procedures at all levels. In this context, all different organizations are integrated at the national level when necessary.

In our country, there is a permanent preoccupation to create the management mechanism of critical infrastructures. The Government created a law[6] which settles a legal and modern frame in this field and creates improved managerial mechanisms designed to uniformly and professionally assure the management of the situations involving the life and health of the people, environment, defense of important material and cultural values, and resumption of normal social and economic life.

The organizational infrastructure liable for fulfillment the Government Emergency Ordinance provisions is constituted of structures from central administration - The National Committee for Emergency Situations, subordinated to ministry of Internal Affairs and coordinated by the prime minister, ministerial committees for emergency situations, the

[5] www.dhs.gov/nipp

[6] Government Emergency Ordinance No. 21/2004 regarding the National System for Emergency Situation Management

general Inspectorate for Emergency Situations from MAI, an operational center at national level and operative centers at ministerial levels. It is obvious that operating such a branchy structure is difficult. The liability is dispersed between institutions, which, as a rule, are not subordinated to each other and follow their own rules, regulations, and political reasons. The decisions cannot be made on time and would have a reduced efficiency in real cases.

Therefore, they appreciate that it is useful to modernize the actual system by creating a governmental organization, unique and permanent, whose purpose is to elaborate the intervention and protection actions in crisis situations, and which is capable to control the means and resources at both the national and local level in order manage them efficiently.

Some aspects should be considered with respect to the structure of this organization the correct definition of critical infrastructures which have to be supervised and protected, depending on the degree of economic development of the country and the existence of real threats; some critical infrastructures, although connected to similar systems from EU, have a lower technological level and the malfunctions that might occur during crises will have a diminished impact; to educate the population to voluntarily participate in eliminating the effects of the crises when they have occurred and eliminating as much as possible the situation in which the population does not participate into any action but waits for the government to intervene; to eliminate the system incompetence caused by excessive politicization and implement rigorous criteria for employment within organization.

The political fight, most of the time independent from real problems of the population, is cynically carried on in critical situations when all efforts should be concentrated to solve them, either to demonstrate the “incapacity” of the government or to justify the “brunt inheritance”, famous phrases in politicians’ vocabulary.

In the case of critical infrastructures whose management is made by information systems, the protection and intervention role must be undertaken by the system administrator who has to permanently analyze the threats and activate protection measures.

BIBLIOGRAPHY

Grigore, Alexandrescu, *Critical infrastructures. Dangers and threats to these. Protection systems.* NDU Publishing House, 2006.

Government Emergency Ordinance No. 98/2010, on the identification, designation and protection of critical infrastructures.

The 26 December Tsunami; Journal La Houille Blanche no. 2/2995.

Damage Situation and Police Countermeasures Associated with Tohoka District – off the Pacific Ocean Earthquake – Japanese National Police Agency, 20.04.2011.

www.dhs.gov/nipp

Government Emergency Ordinance No. 21/2004 regarding the National System for Emergency Situation Management