IMPORTANCE OF INTERDEPENDENCIES IN CRITICAL INFRASTRUCTURES' PROTECTION

Olga BUCOVEȚCHI[1], Petronela Cristina SIMION[2]

In a world in a constant development, with malicious attacks becoming more and more difficult to predict, a one dimensional analysis on critical infrastructures becomes insufficient. In this respect, the authors aim through this article to highlight the importance of taking into account the interdependencies of critical infrastructures. Interdependencies imply the existence of a bidirectional relationship between certain elements of infrastructure; the discontinuity of that relationship jeopardizes the proper functioning of any of the two infrastructures. The authors highlight the energy sector as critical infrastructure and its malfunction's impact on other sectors, especially on IT sector.

Keywords: critical infrastructures, interdependencies, risk assessment, energy sector

1. Introduction

As a consequence of the unprecedented multiplication of the risks, of the hazards and of the threats towards the vital assets of states and international organizations, while increasing the numbers and vulnerabilities, during last decades it led to the settlement of a new concept called "critical infrastructure"(CI).

In all critical infrastructures, advanced information systems are a necessity for the exchange of vital information on the situation of their subsystems exploitation (operation), both within national borders and beyond them, in order to maintain the overall stability of the system. Critical information requires a proper management of infrastructure capacity in transport and energy infrastructure sectors and determines an unprecedented dependence on telecommunications and information infrastructures for the added value reserve.

In general, two infrastructures are considered to be interdependent when each is critically dependent on the other, meaning that each may malfunction due to a damage of other infrastructure. Interdependence is thus defined as a bi-

[1] Asist, PhD Candidate, Dept. of Economical Engineering, Faculty of Entrepreneurship, Business Engineering and Management, University POLITEHNICA of Bucharest, Romania, e-mail: olgabucovetchi@yahoo.com

[2] Lecturer, PhD., Dept. of Industrial Management, Faculty of Entrepreneurship, Business Engineering and Management, University POLITEHNICA of Bucharest, Romania

directional relation between two infrastructures that a state infrastructure unwanted risk is correlated with other risk condition [1]. Interdependencies between critical infrastructures must be subject to particular (specific) assessments, such as the assessment of the digitization of the exploitation of an infrastructure.

There is now a vast interconnected network of systems that are dependent on one other (Fig.1) [2]. There are two concepts in interdependency analysis that we will focus on the coming chapters: interdependencies between the service provider and the service user and interdependencies among infrastructures in a systemic manner.

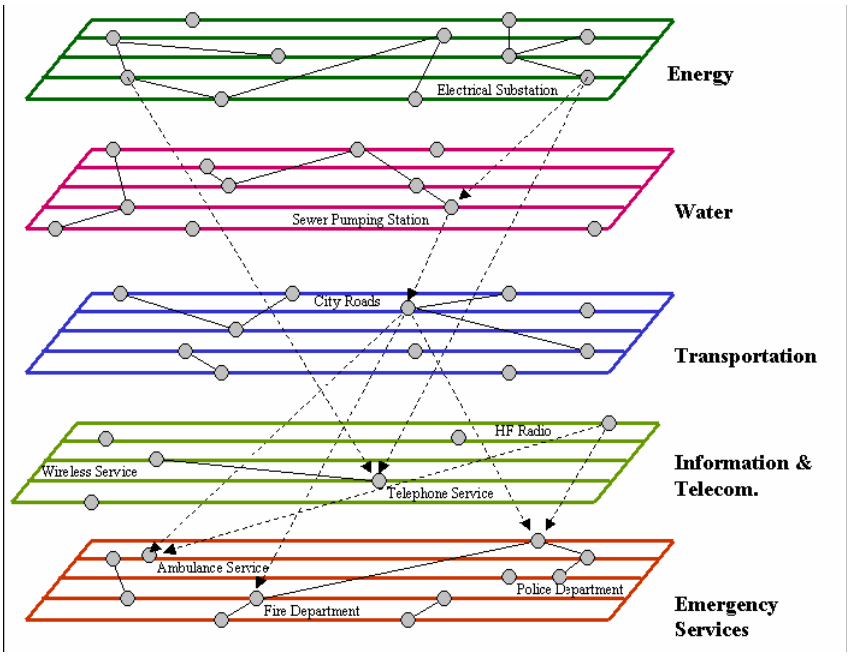

Fig.1 Generic representation of infrastructure interdependencies (Source Pederson et.al. 2006)

2. Interconnections and interdependencies between infrastructures

Among the various dimensions that characterize the interdependencies of critical infrastructures can be included [1, 3]: the type of damage, the operation status, the environment, the response and the connection behavior (Fig.2).

Infrastructures are interconnected not only across national and continental boundaries, but also between infrastructure sectors. The energy sector has increased vulnerability to disruptions information and telecommunication services, and vice versa. Recent studies have shown that in critical infrastructure

protection (CIP) domain many of these interconnections are poorly understood, even within the sectors themselves. Interconnections between infrastructures add a challenge to mastery (treatment) in case of the infrastructure's vulnerability and complexity.

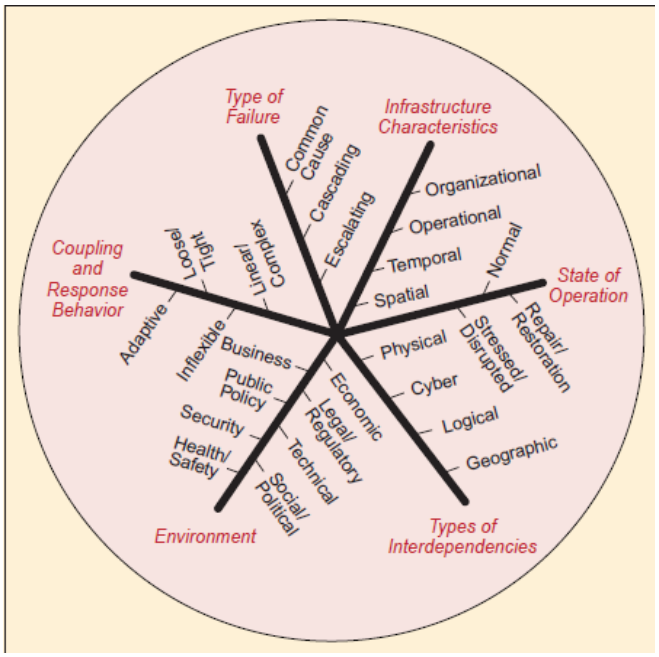

Fig.2 Identifying Understanding and Analyzing Critical Infrastructure Interdependencies (Source:S. Rinaldi and al., 2001)

Other interconnections between infrastructure sectors are created, the so-called convergence phenomena:

- ✓ *Physical convergence* refers to the appearance of multifunctional facilities that provide functions that were provided by various physical networks; for example, the internet services and the television wiring.
- ✓ *Organizational convergence* refers to the emergence of companies that offer multi-utilities, usually operating on the commodity market or selling combinations of utility services; for example: an integrated electricity, gas and water entity.
- ✓ *Market convergence* which refers to converging markets for infrastructure-related services that may be offered by different infrastructures; for example, Internet telephone cable to the Internet via TV or electricity cables.

- ✓ *Spatial convergence* refers to clusters (agglomerations) diverse physical infrastructure corridors and nodes; for example, the glass fiber drawn through the gas pipes or sewer pipes.

Interconnections and interdependencies between infrastructures have been recently recognized as a priority area of research and technological policies. Questions that arise are:

- ✓ How will allocate responsibilities risk management systems interconnected infrastructures?
- ✓ How do you prevent the spread of damage from one infrastructure to another?

Dependencies/Interdependencies in a systemic manner

One example of the catastrophic events of the 21st century given above is somewhat distinguished from others. It is the US-Canada power blackout happened in 2003. It was a man-made error and created a devastating impact not only on the north of the USA, but all around the country. The importance of electricity system and interdependencies between other critical infrastructures had become evident [4].

Cleveland experienced its worst water crisis in history as the blackout shut down all major pumping stations, which serve more than 1 million residents. The National Guard had to tank in thousands of liters of drinking water until taps flowed again. In Detroit five days after the outage tap water was still undrinkable. In major cities (e.g. New York) streams of raw sewage began to flow into surrounding waterways posing health and environmental hazards.

Another example can be given from Kyoto Earthquake Japan which is pointing out dependencies and interdependencies to transportation system. The economic cost of a disaster can be estimated by disruption in transport and other systems. For example, in Niigata-Chuetsu, the earthquake in 2004 led to an estimated economic loss in infrastructure of 1,200 million Yen in highways, railroads, rivers and bridges, and 100 million Yen in power, gas and water services, amongst others. The smoothness in the recovery of the infrastructure also depends on the ability of the transport network to recover rapidly. For example, the power supply did not recover rapidly in Niigata-Chuetsu as it was situated in a remote region without good access and was down for over 30 days. This was a much longer period than in Hanshin-Awaji which is more accessible [5].

Problems can cascade through interdependent infrastructures, causing unexpected and increasingly more serious failures of essential services. Interconnectedness and interdependence make these infrastructures more vulnerable to disruption or destruction.

Critical infrastructures have become more dependent on common information technologies, including the internet and space-based radio-navigation and communication.

Dependencies/Interdependencies between Service Provider and User

Catastrophic terrorism, natural disasters, or inadvertent failures of large-scale public services are not so distinct from each other and they shouldn't be addressed and separately managed. Auerswald et al. [6] conclude that national, regional or municipal governments are still not able to reduce the likelihood or the consequences of such catastrophic events on the contrary to common conventional wisdom.

After the experiences of theses catastrophic events of the 21st century the main picture that governments face is that the new economic world is so complicated that actors of this game are extremely interrelated with each other. Most of the publicly held and governed infrastructures like bridges, airports, tunnels are used by trucks, airplanes, ships are privately held[6]. In the United States, it has been estimated that more than 80 percent of the physical assets like shopping malls, office buildings, theaters, factories, energy installations, and airlines that might be targeted by terrorists or natural disasters are owned by private business [7].

Creation of US Department of Homeland Security can be seen as a response to deal with interdependencies. It was established on 1st of January 2003 where task is simply to protect the nation against terrorist attacks and natural disasters. One of their major works was to identifying and analyzing critical infrastructures and put them in a place in the national protection plan.

In their report to congress Moteff et al. states that there are number of ways the government can prioritize critical infrastructures [4]. First, not all elements of a critical infrastructure are critical. Additional study will be necessary to identify those elements that are the most critical. Other approaches include focusing on vulnerabilities that cut across more than one infrastructure, interdependencies where the attack on one infrastructure can have adverse effects on others, geographic locations where a number of critical infrastructure assets may be located or focusing on those infrastructures belonging solely to the federal government or on which the federal government depends on [8].

However, in their book Auerswald et al. argue that, aftermath of the 9/11 and Madrid attacks national governments are still not working closely and effectively with relevant private enterprises in order to minimize the probability and impact of future attacks [6].

Chain dependencies may lead to the unforeseen domino effects, whereby disruption of one infrastructure may become a source of disturbance to other infrastructures. A clear understanding of the extent of the interdependence is crucially important for dealing with such cascading effects, along with the

application of effective emergency preparedness measures [9].Electrical power supply is seen as the single factor underlying all Information and Communication Technology (ICT). Disruption to power supply therefore has the potential to cause large-scale interruption of these critical ICT services with cascading effects into other sectors of the economy. Above power supply, ICT network-infrastructure consists of information transmission facilities such as telecommunications equipment, glass fibres and cables, satellites, radio and TV transmitters. In addition, these facilities themselves also rely on ICT hardware and software components for monitoring and control. [9].

The frequency and load control process is based on SCADA systems which are operated through the Transmission System Operator (TSO) control room. In general, the SCADA works with Wide area network (WAN) on the remote objects. In addition, these objects can also be peripherally operated by personnel on site which receives information through communication lines.

The coordination process between the TSOs of control areas mainly takes place through an "electronic highway", which is implemented as a secure private network. In addition, voice and e-mail communication can take place through mobile/landline telecommunication and or internet.

The frequency / load control processes could also be interrupted by failures in the SCADA systems, causing incorrect switching of lines and/or transformers, which might lead to overloads and cross-border cascading effects, triggering in the worst case separations of the interconnected system and black-outs. But in this case any cascading effects and separation of the system would occur only accidentally, because the SCADA system itself does not "know" which lines and transformers are critical in a current state of the overall system to trigger the worst case.

3. Case study on electricity sector

The electric power network relies on the gas supply system, which provides fuel for generators; on the rail network, which transports other fuels such a coal; and increasingly on ICT systems, which control and manage electricity systems and markets [10]. There is less dependence on urban water systems, since cooling water for power plants is typically drawn from different sources.

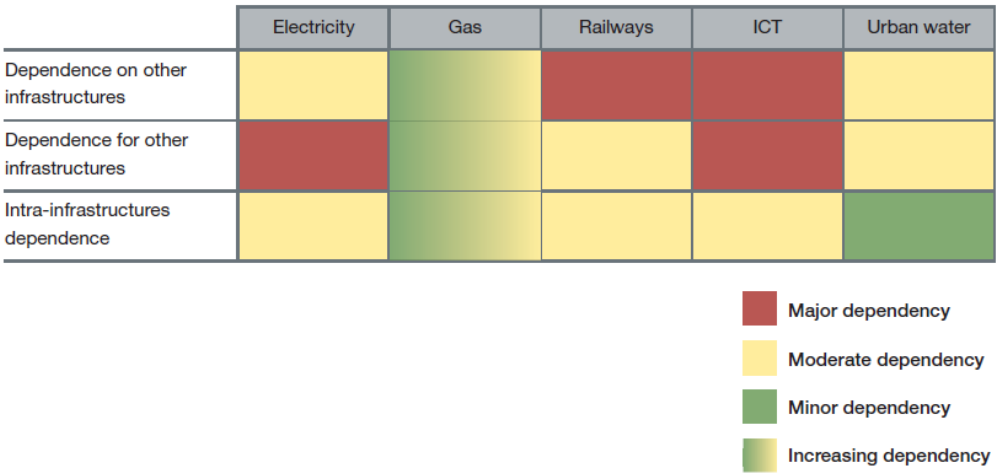

Fig.3 Interdependences of electricity sector
(Source: IRGC, Managing and reducing social vulnerabilities from coupled CI, 2006)

After identifying the systems required to perform the mission, it is important to trace the relationships among critical systems. The result will be a system functional diagram illustrating how the critical systems interconnect. From the system interconnection schematic it is sometimes useful to develop a fault tree representation of the logical dependence of system mission on supporting systems. Understanding system interdependencies enables an evaluation of cascading failures wherein failure of one system can have downstream effects on one or more additional systems. System functional and fault diagrams are the basis for computer analysis of system threat response. An important related consideration is whether critical systems have back-up (or "fail-over") systems in place, or replacement spares readily available should they fail.

Increasing interdependence among infrastructure service providers intensifies the problem of assuring failure-free operations. Interdependent systems are only as reliable as their least reliable part as the risk migrates to the weak links. While it is difficult to know the vulnerabilities of other organizations/facilities both upstream and downstream, it is prudent to consider the effects of outages of both upstream and downstream organizations/facilities [11]. Communication among interdependent organizations can help raise the general robustness of the complex.

a. Downstream Dependencies. The effects of the debilitation of your facility will cascade to other facilities and organizations. Start by developing a complete list of facilities and organizations dependent on your mission. Understand the extent to which outside organizations depend on your products and services. There are time factors involved here as well. Outages of limited duration may not be noticed. Determine how long it will be before other dependent organizations become aware of your

incapacitation. Identify the outage time that will result in dependent organizations becoming unable to perform their missions. Review of past downtime incidents are very instructive in this regard.

b. Upstream Dependencies. Your facility depends on services from other "*resource*" facilities. Again, it is important to recognize and list these.

Identify any single-supplier organizations whose products and/or services are not duplicated by competitors. Consider threats that might affect upstream organizations and try to estimate the duration of their downtime and effects on your operations under possible threat and hazard conditions.

Nowadays, when talking about the electricity sector as a CI sector, it became mandatory to talk also about three elements regarding this field: Smart grid, grid dynamics and regulatory requirements.

- Smart Grids. This topic is seen as a next-generation technology for electricity supply and its management. It is based on a general two-way flow of electricity and information based on arrangements of metering systems and sensors which measure and control energy flow from energy supplier to the customers in order to optimize and adjust energy production and consumption in a limited area and avoiding energy transmission over long distances. This technology implies new point of attacks and vulnerabilities which have to be addressed.
- Grid dynamics. Due to the increases in power trade and construction of wind farms (offshore) the Union of the Coordination of the Transmission of Electricity (UCTE) grid is exposed to a transport function for which it was not designed. Countermeasures lead to high loads on existing lines and increasing switching operations. Regional and intermittent generation by wind farms entail additional network dynamics which are sometimes out of current control possibilities. Some TSOs try to cope with these new phenomena by wide area monitoring (real time data for load flow, angle and heat).
- Regulatory Requirements. Segregation of business activities (e.g. of production and transmission) lead to longer coordination processes in case of emergency. In the course of the unbundling of production and network operation the industry is going to physically separate the dispatch control rooms from the transmission system operation control room, and thus the industry is establishing new control and communication infrastructures and coordination processes.

The following trends [10] will have a significant impact on the energy sector: the increased connectivity between networks, the increased wireless networks and the broadened use of commodity IT platforms.

4. Conclusions

It is impossible to ignore the interdependencies as not having a bird-eye-view on the entire business can drive to the total failure of the activity. Interdependencies may lead to unforeseen ripple effects, where the disruption of one infrastructure becomes a source of disturbance to other infrastructures. Application of effective emergency preparedness measures is therefore critically important for dealing with cascading effects.

The dependence on information systems introduces security issues that can have a significant impact on the resilience and reliability of critical infrastructures, regardless of whether the supporting systems are centralised, stand alone or embedded.

Insider attacks, either errors or sabotages, remain amongst the most significant threats, together with a risk of organisational failures and internal interdependencies.

REFERENCES

[1] *Gheorghe, A., Masera, V., Weijnen, M., De Vries, L.* „Critical Infrastructures at Risk. Securing the european electric power system", Published by Springer, 2006

[2] *Pederson P., Dudenhoeffer D., Hartley S., Permann M* "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research" Idaho National Laboratory August 2006

[3] *Rinaldi S., Peerenboom J., and Kelly T.,* "Identifying Understanding and Analyzing Critical Infrastructure Interdependencies," IEEE Control System Magazine, pp. 11–25, 2001

[4] *Moteff J., Copeland C., and Fischer J.* "Critical Infrastructures: What Makes an Infrastructure Critical?" Report for Congress January 29, 2003

[5] *Hirokazu Tatano,* "Some Issues of Disaster Risk Governance: Focusing on the Inter-Dependence of Infrastructures" IRGC's General Conference on 'Implementing A Global Approach to Risk Governance' Beijing September 2005

[6] *Auerswald P.E., Branscomb L.M., La Porte T.M., Michel-Kerjan E.O.* "Where Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge", "Seeds of Disaster, Roots of Response" Cambridge University Press 2006, 3-19

[7] ***President's Council of Advisors on Science and Technology "The Science and Technology of Combating Terrorism Report", July 2003

[8] *Dunn M. and Wigert I.* "The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries" eds. A. Wenger and J. Metzger, Swiss Federal Institute of Technology, Zurich 2004

[9] *Luiijf, I. and Klaver, M.* "In bits and pieces/ Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society" INFODROME. 2000

[10] ***International Risk Governance Council (IRGC) "White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures" October 2006

[11] *George H. Baker*, "A Vulnerability Assessment Methodology for Critical Infrastructure Sites" DHS Symposium: R&D Partnerships in Homeland Security. Boston, Massachusetts. Apr. 2005. Available at: http://works.bepress.com/george_h_baker/2