THE CYBER SECURITY OF CRITICAL INFRASTRUCTURES IN AN INCREASINGLY CONNECTED WORLD

LtCol. Eng. Vasile Florin POPESCU, PhD*

In an increasingly connected world, critical infrastructures have become more vulnerable than ever to cyber security threats, whether they come from national states, criminal organizations or individuals. This new vulnerability stems from fundamental changes in the technological systems of organizations (government and private). In this regard, the Virtual Critical Infrastructure of any organization / nation represents an arena where security is absolutely imperative. Cyber protection has become crucial in every sector of activity, and the absence of measures to protect critical infrastructures threatens to cause huge damage to the functioning of the company.

Keywords: critical infrastructures; cyber space; cyber threats; vulnerabilities; information and operational technology systems.

Aircraft hijacked from the normal course. Underground trains stuck in tunnels below cities. Broken dams flooding cities. Power cuts. Blocked telecommunications. Unusable 112 emergency calls. These moments of chaos and panic and other potential consequences of attacks on critical infrastructure can at best only cause these drawbacks, and in the worst case, they can lead to loss of human life or widespread destruction.

Nowadays, about half of the world's population lives in urban areas and it is assumed that the urbanization process will accelerate, so that only one third of the planet's inhabitants will live outside urban areas by 2050[1]. This development raises a number of challenges that also influence infrastructures, whose reliable and efficient functioning will determine how cities are able to meet the demands of quality of life[2]. Some of these infrastructures are called "critical" because the welfare of the society is fundamentally based on their reliability. They can be understood as the fundamental elements of the sustainability of society, the security and security of supply. Critical infrastructures offer people access to a wide range of goods, the availability of which is essential for the resilience of communities[3,4].

Etymologically, according to Oxford English Dictionary, the term infrastructure is a combination of the Latin prefix "infra" with the meaning of "under" and the suffix "structure", which shows how a mechanism is constructed. The association of the term "critical" with that of "infrastructure" defines that type of infrastructure that disrupted can lead to major damage.

The critical character of the infrastructures is given by:

- Their uniqueness;
- The vital character in the functioning of the economic, social, political, military, information systems, etc ...);
- Sensitivity to changes;
- High vulnerability to threats from the external environment.

Depending on their importance for the functionality of the systems and processes, the infrastructures are divided into three categories[5]:

- Common infrastructures;
- Special infrastructures;
- Critical infrastructures.

Critical infrastructures are divided into two important categories[5]:

- Physical:
  - International;
  - of the economy of the states;
  - of the different industrial sectors;
  - of companies / companies;

***Ministry of National Defence**
e-mail: *popescuveve@gmail.com*

- of projects;
- of air and rail and naval transport;
- of the financial system;
- of the house, of the town/village, of the country and of the continent;
- military;
- of the public order system;
- of the intelligence and security system of the state;
- of the health and protection system of the citizen, family and community.

- Virtual:
  - of the communication systems;
  - of networks and databases;
  - of cyber space.

In an increasingly connected world, critical infrastructures have become more vulnerable than ever to cyber security threats, whether they come from national states and criminal organizations or individuals. This new vulnerability stems from fundamental changes in the technological systems of organizations (government and private). Such organizations - army, police, firefighters, providers of medical services and utilities, banking systems, transport systems, etc ... act with two types of technological systems: information technology systems and operational technology systems.

Information technology systems provide basic functions of the office, such as: email communication, payroll, human resources, etc., while operational technology systems control the physical equipment and personnel essential to fulfill their mission. In the past, operational technology systems consisted of stand-alone systems that made them secure. Now, systems operating technology systems run on the same software and hardware platforms commonly, known as IT systems. These systems are well known to hackers and are therefore significantly less secure.

What led to this convergence of information technology systems with operational technology systems? Here are some examples:

A homeowner remotely adjusts the thermostat to his home to lower the temperature while on vacation. A doctor visualizes the insulin use of patients on a desktop computer. Companies remotely monitor the condition and location of trains, buses and trucks; oil and gas flow through pipelines; or the use of water or electricity to manage these services effectively. While the technologies in these examples improve our lives, they can make us vulnerable at the same time.

I am saying this because as the number of interconnected devices continues to grow, the number of potential access points for hackers to disrupt critical infrastructure also increases. In this regard, the Virtual Critical Infrastructure of any organization/nation represents an arena where security is absolutely imperative. Cyber protection has become crucial in every sector of activity, and the absence of measures to protect critical infrastructures threatens to cause huge damage to the functioning of the society as a whole.

Virtual or cybernetic space is a set of means and procedures, based on information and communication technology (ICT), and consist of hardware, software, internet and information services, and control systems becoming critical infrastructure for the socio-economic activity of any nation, a transnational organization or project. Different dictionaries and encyclopedias define cyber space as follows:

- Cyber-space: a computer network made up of a global network of computer networks, that use TCP/IP network protocols to facilitate data sharing (Source: Online Romanian Dictionary);
- Cyber space is the electronic computer network environment where online communication takes place. Wikipedia, http://en.wikipedia.org/wiki/Cyberspace[6].
- A metaphor to describe the non-physical terrain, created by computer systems: Online systems create a cyber space where people can communicate with each other, perform research, or simply buy things. http://www.webopedia.com/TERM/C/cyberspace.html[7].
- Cyber space is a field characterized by the use of electronic devices and electromagnetic spectrum to store, modify and exchange data through network systems and associated physical infrastructures. In fact, cyberspace can be considered as the interconnection of human beings through computers and telecommunication, regardless of geographic position.http://searchsoa.techtarget.com/definition/cyberspace[8].

The US Government defines the slightly wider cyber space. The Presidential National Security Directive no. 23 and 54 define cyberspace as the interdependent network of information

technology infrastructures, including the Internet, telecommunication networks, computer systems, users and those who control critical industries. The common use of the term also refers to the virtual information environment and interactions between people.

The definitions offered by Webster, Wikipedia, or the Oxford Dictionary are not absolute and comprehensive enough. The concept of virtual space has expanded in the meantime, including trade, finance, energy, stock exchanges and so on. The objectives of the attacks in the virtual environment can be classified into three major groups:

- the public sector and government agencies;
- the private sector, mainly critical infrastructure operators;
- citizens.

Cyber attacks can be classified, depending on their source and impact, as follows:

- *Attacks sponsored by states*

The real world and physical conflicts have expanded into the virtual world of cyberspace. In recent years, cyber attacks have been detected against critical country infrastructures and specific targets. Some examples that are widely known by the public are: Estonia's cyber attack in 2007, which led to the temporary deactivation of a large part of the critical infrastructure of the Baltic countries, the cyber attack launched by Russia against Georgia in 2008 as a prelude to earthquake-like invasion, the Stuxnet case with cyber attacks against SCADA systems, the Duqu's case of cyber attacks against industrial organizations, the cyber attacks suffered by the US Government's classified networks by hackers in Chinese territory. In recent years, some states have invested considerable economic, technical and human resources in developing persistent advanced threats (AAP), aggressively attacking and choosing very specific goals, in order to maintain a steady presence within networks of possible victims. AAP attacks are very difficult to detect because they use techniques and components that are specifically designed to infiltrate and remain in the network without being detected.

Attacks sponsored by private organizations

The objective of many private organizations is to obtain industrial and economic secrets from other competing organizations, and this type of attack is often executed with government support;

- *Attacks of organized crime groups*

Organized crime gangs, also known as computer gangs, began to work in cyberspace, exploiting the possibility of anonymity that this domain offers. The objective of these types of gangs is to obtain sensitive information for their subsequent use for fraud and for significant economic gains.

- *Hackers*

With the advent of the Internet, but especially in recent years, hacker activities have become one of the greatest threats to governments and organizations of all kinds. The principles of this aggression are the anonymity and the free distribution of information through cyber space, essentially via the Internet. Their mission is to "attack" the cyber space of people, companies, projects or other organizations that violate any of their principles or interests. This implies that the cyberspace of governments in most countries around the world, banks, telecommunications companies and critical infrastructure providers, Internet service providers and ultimately all cyberspace are likely to be hacked with the goal to steal sensitive information.

• *Attacks of privileged (in-house)*

These groups are one of the greatest threats to the cyberspace security of nations, companies /projects because they are often an integral part of all the attacks outlined above ... from a spy infiltrated by a state or an employee who work for gangs of terrorists or cyber criminals, dissatisfied employees, etc.

Conclusions and recommendations

The need to stimulate cyber defense for critical infrastructures is clear. However, the question now turns into: How do we get there? In this regard, we have developed some recommendations to contribute to effective collective actions.

- Developing a national strategy for cyber education: to truly protect critical infrastructure, we must have qualified people. Therefore, it is necessary for cyber education to become a higher priority in the educational process. Romania does not have a strategy of education in the field of cybersecurity, that will feed and finance national centers of excellence in the field of cybersecurity.
- Another recommendation is trans-organizational mentoring and knowledge transfer.

Organizations with less cyber security experience or smaller cybersecurity teams can learn from the experience of their more experienced colleagues. Larger organizations should also encourage their experts to participate in industry associations, public-private partnerships and regional organizations, which provide all opportunities for formalizing inter-organizational guidance and knowledge transfer.

- Creating better strategies for sharing information between the government / state and the private sector: cyber security experts seem to agree that for an optimal level of security in all sectors, cooperation is essential.
- Performing scenarios exercises for potential crises: when it comes to critical infrastructure, a real disaster is not the time to learn from mistakes. Such preparation must take place in advance, in crisis scenarios exercises that simulate how a response team would deal with an unexpected incident.

NOTES:

1 Rizea M. et al. UN (United Nations), *World Urbanization Prospects: The 2018 Revision*, Key Facts, 2018. Available online: https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf (accessed at 10 November, 2018).

2 Riffat S., Powell R., Aydin D., *Future cities and environmental sustainability. Future Cities Environ*, 2016, 1–23 [CrossRef].

3 Hay A.H., Willibald S., *Making Resilience Accessible. Access: An Enabler of Community Resilience Southern Harbour,* 2017, available online: https://www.southernharbour.net/assets/docs/SH_Access20WhitePaper_2017_0307%C6%92.pdf (accessed at 14 January, 2019).

4 Hay A., *Surviving catastrophic events: Stimulating community resilience*. In Infrastructure Risk and Resilience:Transportation; IET: Stevenage, UK, 2013, pp. 41–46.

5 Alexandrescu G., Văduva Gh., *Infrastructuri critice. pericole, ameninţări la adresa acestora. sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.

6 http://en.wikipedia.org/wiki/Cyberspace

7 http://www.webopedia.com/TERM/C/cyberspace.html

8 http://searchsoa.techtarget.com/definition/cyber space

BIBLIOGRAPHY

Rizea M. et al. UN (United Nations), *World Urbanization Prospects: The 2018 Revision*, Key Facts, 2018. Available online: https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf (accessed at 10 November, 2018).

Riffat S., Powell R., Aydin D., *Future cities and environmental sustainability. Future Cities Environ*, 2016, 1–23. [CrossRef].

Hay A.H., Willibald S., *Making Resilience Accessible. Access: An Enabler of Community Resilience Southern Harbour,* 2017, available online: https://www.southernharbour.net/assets/docs/SH_Access20WhitePaper_2017_0307%C6%92.pdf (accessed at 14 January, 2019).

Hay A., *Surviving catastrophic events: Stimulating community resilience*. In Infrastructure Risk and Resilience: Transportation, IET: Stevenage, UK, 2013.

Alexandrescu G., Văduva Gh., *Infrastructuri critice. pericole, ameninţări la adresa acestora. sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.