Annals of the Academy of Romanian Scientists
Series on Engineering Sciences
ISSN 2066-8570 Volume **2**, Number **2**/**2010**

IT&C DIMENSION OF THE CRITICAL INFRASTRUCTURE IN THE MODERN SOCIETY

Cristea DUMITRU[1]

Rezumat: *Deşi binomul comunicaţiile şi tehnologia informaţiei este de provenienţă foarte recentă relativ la scara istoriei umanităţii, apreciem că de-a lungul dezvoltării societale a omului, existenţa şi calitatea comunicării au fost determinante pentru succesul evoluţiei umane. Iniţial, comunicarea s-a realizat îndeosebi prin intermediul limbajului şi scrisului, acţiuni ce aveau drept scop transmiterea de informaţii. O dată cu inventarea mijloacelor moderne de comunicare (telefonul, radioul, reţelele de calculatoare), schimbul de date şi informaţii a putut fi realizat aproape instantaneu la distanţe foarte mari şi într-un volum foarte mare. Beneficiile aduse omenirii de comunicaţii şi tehnologia informaţiei sunt indiscutabile şi au devenit un important factor de progres. Societăţile ce deţin reţele de comunicaţii şi calculatoare extinse sunt axiomatic şi cele mai dezvoltate.*

Abstract: *Although the information technology and communications binomial has a very recent origin in the humankind history, we consider that the existence and the quality of the communication are decisive for the success of the human evolution, throughout its social development. Communication was initially performed by the means of language and writing, two actions with the purpose of transmitting information. Once the modern means of communication were invented and developed (phone, radio, computer networks), the flows of data and information have been done almost in real time at very long distances and in great capacity. The advantages brought to the humankind by the information technology and communications are beyond any doubt and turn into an important ingredient of progress. Societies with extended networks of computers and communications are axiomatic the most developed.*

Keywords: IT&C, information technology and communications, critical infrastructure, cyber attacks

1. Introduction

As the technological development inflicted the people's addiction to the computers and means of communications, both in personal and economic activity, the IT&C field became important and a sensitive resource for the modern society. We can assert that the information technology and communications come across the most of the activities carried out by the present-day persons, thus the security of the IT&C field is one of the intrinsic condition for the normal and safe social life, and one of the infrastructure element of the society.

[1]Prof., PhD, National Defence University, Bucharest, Romania, corresponding member of the Academy of Romanian Scientists, Military Sciences Section, AFCEA (Armed Forces Communications and Electronics Association) member, Lieutenant General (ret.), former Chief of Romanian J6 (Directorate of IT&C in General Staff) - (e-mail: dumitru.cristea@computerland.ro).

Information technology and communications services and networks provide the technical support of every developed country and are vital to citizens, businesses and governments. It is inour intention to assess the IT&C importance since they are often referred to as critical infrastructure. Information infrastructures like telephone lines, fibre optic cables and computer networks rule our lives, and they have to be safe. Large parts of the economy are relying on this. Many services and processes have become increasingly dependent on the functioning of information technology and communications networks. As these networks tend to be decentralised, highly interconnected and interdependent, failures of these infrastructures could cascade and spread beyond national borders. [1]

2. Critical Infrastructures – Concept Evolution

The national infrastructures have a vital nature, and as a consequence their spoliation or destruction could have a devastating or destabilizing impact on the national security. By the middle of the twentieth century the national infrastructures were called objectives or infrastructures of special importance. The very first studies on the national infrastructures have identified the objectives believed to be critical since the ’80s, and the critical infrastructure collocation being officially used on July 1996, when the US president ordered the “Executive Order 13010 on Critical Infrastructure Protection”. The preamble of this document explains that “*certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States*”.[2] Thereby, it is considered that these critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. In the same year, the established President’s Commission on Critical Infrastructure Protection considered that the security, economy, and even the survival of the industrialized world depend on three interdependent elements: energy, communications and computers.

The national and international security is greatly related to the critical infrastructures of the society. However, the critical infrastructures are vulnerable to the increasingly sophisticated means of attack pointed to them. The methods to protect the critical infrastructures are comprehensively analyzed in the special literature. In the study of this field two facts are accepted: it is almost impossible to ensure the complete protection of a critical infrastructure, and second, there is no unique universal solution to solve this issue.

The critical infrastructures represent the most sensitive and vulnerable field of every system and process. The vulnerability of the critical infrastructures could

be explained by the difficulty to ensure a proper protection, during the project or finalization phases, and by the increment of the programmed pressures with direct or indirect, intended or random actions on them. In this case, the vulnerability is direct proportional with the role played by the critical infrastructures. Consequently, regardless their degree of protection, the critical infrastructures will always have a high level of vulnerability because, as a general rule, they are the first aimed when a system or a process is intended to be destabilized or destroyed. The identification, optimization, and security of the critical infrastructures are the indisputable priority of both managers of systems and processes, and their foes, namely the ones who want to destabilize and destroy the aimed systems and processes. As a rule, after the 9/11 terrorist attacks on World Trade Center and Pentagon, it is assumed that the infrastructures are or could become critical in relation to terrorist attacks or other threats, specially asymmetric threats. This is just an aspect or criterion used to identify the critical infrastructures. Yet, there are more other criteria that are related both to the stability and functionality of the systems and processes, and to their relations with the external environment. Therefore, in our opinion, the analysis of the critical infrastructures issue should keep account of all dimensions and implications for the stability and functionality of the systems and processes, as well as of the causal links that could generate or influence their dynamic.

The member states of the European Union take decisive steps in the last years toward the establishment of a common way of action in order to protect their objectives of strategic value. Generally, the communitarian states decided to introduce in the category of critical infrastructures the following: telecommunications, water and energy sources, networks of food production and distribution, health institutions, transportation, financial and bank services, and defense and public order institutions (army, gendarmerie and police).

At its reunion in June 2004, European Council asked European Commission to prepare an overall strategy to enhance the protection of critical infrastructures.

The associate risks to potential terrorist attacks over European critical infrastructures increased. It is considered that the consequences of such attacks could vary. A cyber attack is estimated to cause a few or no victims, but could drive to the interruption of the vital infrastructures operation. For example, a cyber attack against the telephone network could disrupt the phone calls for the time needed to fix the problem, with unpredictable chain effects. [3] However, there is another perspective over the attacks of the critical infrastructures. An attack at the command and control systems of the chemical installations or gas networks could inflict many victims and significant damages. Moreover, the effects could multiply and spread uncontrolled. An attack at the power grid could have very big effects, both over the normal operation of the enterprises, computer

networks, communication networks etc., and over the medical care equipments which are vital for ill people found under surgery operations or in monitored surveillance in the facilities without own power sources. The power breakdowns happened in the last decade in North America, South America or Europe shown how greatly vulnerable the power infrastructures are.

According to the European definition, the critical infrastructures are "*those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the member states. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services*" [4].

In the European view the critical infrastructures comprise:

- Installations and networks in the energy sector (specially the producing installations of electricity, gas and petroleum, storing installations and refineries, system of transport and distribution);
- Information technology and communications (telecommunications, radio broadcasting systems, information software and hardware, networks including the Internet etc.);
- Finance (banking sector, investments and stock market);
- Health care sector (hospitals, equipments for ill people care and blood stocks, laboratories and pharmaceutical products, emergency, search and rescue services);
- Food sector (security, means of production, distribution and agro-alimentary industry);
- Water supply (reserves, stocks, water treatment, and networks of distribution);
- Transportation (airports, harbors, crossing installations, railways, massive transit networks, traffic control systems);
- Production, stocking and transport of hazardous products (radiological, nuclear, biological and chemical products);
- Administration (basic services, installations, network of information, actives, important locations, national monuments). [5]

These critical infrastructures belong both to the public sector and private sector. Hence, according to European Commission, the public authority must to assume the responsibility for the consolidation and protection of these critical infrastructures.

The Romanian legislation regarding the definition and protection of the critical infrastructures has rather a discontinuous nature, without a systemic and integrating approach. Analyzing the existing conditions from the perspective of the Romania's member quality in European Union, we consider that the protection of the national critical infrastructures could be best provided through legislative harmonization, the proper definition of the Romanian critical infrastructures dependences and inter-dependences in accordance with the European Union conception, as well as the commitment of the Romanian decision makers and experts in order to define and implement the European policies and strategies from the critical infrastructures field.

3. IT&C Dimension of the Critical Infrastructure

In our opinion, the IT&C dimension of the critical infrastructure in Romania should be made of the following systems and services:

- Information systems and networks;
- Command, automation and instrumentation systems;
- Mobile and fixed telecommunications services;
- Radio communications and navigation services;
- Satellite communications services;
- Radio broadcasting services.

The IT&C domain is essential for all areas of the society. The economical structures are based on the information technology and communications both in the production and direct commerce, and in the efficiency of the internal processes. This critical infrastructure of the society is an essential component of the innovation and determines around 40% of the productivity growth. The use of the information technology and communications is also generalized in the activity of the public administration by the employment of e-government services at every level, and by using the innovative solutions in energy and health fields. Last but not least the citizens rely ever more on the information society specific services.

Information technology and communications is currently the most important industrial sector of the transition from the society based on mass production to the Information Society defined by globalization, flexibility, and mobility. The unique impact of the information technology and communications consists of its role played for the transformation of the economy and society as a whole. The technologies and global networks of communications transform the economic activities, leading the way to the growth of labor productivity, to new economic opportunities, and to new jobs.

IT&C dimension of the critical infrastructure faces risks caused by the attacks conducted by the human factor, natural catastrophes or technical deficiencies, risks that are not always well acknowledged.

4. Impact of Cyber Attacks on IT&C Critical Infrastructure

The cyber attacks evolved to an unprecedented level of complexity. Simple experiments become today complex activities developed for political reasons or in order to obtain economical profits. The extended cyber attacks against Estonia, Lithuania and Georgia are the most publicized examples of a largely spread trend. The huge number of viruses, information worms and other forms of malicious software, the expansion of botnets and continuous increase of the spam number confirm the seriousness of the problem.

Cyber attacks can include the spread of propaganda, industrial espionage that weakens a nation's global competitive advantage, the clandestine modification of sensitive data on the battlefield, or the disabling of a country's critical infrastructure – power, water, fuel, communication, or commercial assets that are essential for the functioning of a society and economy. [6]

Related to the cyber attacks issue we would like to depict the Estonian case which could be considered as being representative.

Estonia, a country of 1.4 million people, including a large ethnic Russian minority, is one of the most wired societies in Europe and a pioneer in the development of "e-government". Being highly dependent on computers, it is also highly vulnerable to cyber-attacks. The cyber attacks were clearly prompted by the Estonians' relocation of the Soviet World War II memorial on April 27th, 2007. The remains of soviet soldiers, on top of which the monument had been constructed, were also to be exhumed and reburied in a cemetery. This decision led to street riots in Tallinn and a siege on the Estonian embassy in Moscow by people who claimed that the government in the ex-Soviet country was being led by Fascist sympathizers. Ethnic Russians staged protests against the removal, during which 1,300 people were arrested, 100 people were injured, and one person was killed. [7]

The crisis started with a wave of so-called DDoS, or Distributed Denial of Service, attacks, where websites are suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers running the sites. The attacks have been pouring in from all over the world, but Estonian officials and computer security experts say that, particularly in the early phase, some attackers were identified by their internet addresses, many of which were Russian, and some of which were from Russian state institutions. The main targets have been the websites of: the Estonian presidency and its parliament, almost all of the country's government ministries, political parties, three of the country's six big news companies, two of the biggest banks, and firms specializing in communications. The attacks disrupted the Internet connections across the country and, more importantly, affected the activity of

financial and government institutions and websites, leading to significant losses. It is not clear how great the scale and the damages of the attacks have been. Probably the most exposed critical infrastructure of Estonia, a NATO and EU member state, was disrupted by a brand new weapon – the cyber attack.

The anonymity enjoyed by cyber aggressors adds a deeply complicating dimension to the nature of the threat. Unlike the telephone system, which has an effective tracking and billing capability based on the need to charge users, the Internet was designed as an open and robust system for the sharing of information, and therefore has no standard provisions for tracking or tracing the behavior of its users. Some experts suggest that it may never be possible to retrofit any mechanism to completely eliminate the threat posed by the omission of tracking features in the Internet's initial design.

The cost of cyber criminality is now estimated as being between $ 100 billion and $ 1 trillion annually (although banks and other major companies are reluctant to release figures about the losses they sustain). [8] Organised crime gangs are running profitable operations involving programmers writing malicious software and viruses, and computer security experts have even talked of the commercialisation of cyber crime – the creation of a marketplace where hackers openly tout their services to the highest bidder – potentially closing the gap between hackers and political actors without computer skills. Latest reports confirm that cyber criminality is increasing with the pressures and opportunities presented by the global economic downturn.

Cyber attacks often cross multiple administrative, jurisdictional, and national boundaries. Countries with weak domestic legislation on Internet crime have become safe shelters for cyber attackers, and it is unlikely that anything other than concerted international pressure to adopt and implement effective laws will be successful in countries where the government has financial ties to cyber attackers, or has a political agenda to protect them. There is now widespread recognition that legal efforts to deter future attacks must form a key aspect of any cyber defence strategy with the ultimate goal of IT&C critical infrastructure protection.

Conclusion

The high level of dependence to information technology and communications, their interconnection and trans-border interdependence with other critical infrastructures, as well as the vulnerabilities and threats they confront with, dramatically increase the need to approach the problem of their security and resilience from a systemic perspective, as the first line of defence against the cyber attacks and technical shortcomings.

The diversity, openness, interoperability, easy use, transparency, the possibility to audit different components, and the competition featured by the IT&C represent engines of evolutions in the security field of the critical infrastructures.

Out of what we have presented so far, without the intention of comprehensiveness, we would like to conclude with the obvious fact that the IT&C field is one of the critical infrastructures of the society, both as a single element and viewed from a systemic inter-relational perspective, representing one of the dimensions which ensure the viability of the contemporary modern society. Furthermore, the human society that progresses toward an Information Society or a Knowledge Society will directly depend on the IT&C field, this one keeping on its status of critical infrastructure.

REFERENCES

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM(2009) 0149 final, *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, (Brussels, Belgium, 2009).

[2] Executive Order 13010 of July 15, Federal Register, Vol.**61**, No.138, *Critical Infrastructure Protection*, (Washington DC, USA, 1996).

[3] [4] Communication from the Commission to the Council and the European Parliament, COM(2004) 702 final, *Critical Infrastructure Protection in the Fight Against Terrorism*, (Brussels, Belgium, 2004).

[5] G. Alexandrescu, G. Văduva, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, (Editura Universității Naționale de Apărare, București, România, 2006), p.16.

[6] , [8] NATO Parliamentary Assembly,, Committee Reports, 173 DSCFC 09 E bis, *NATO and Cyber Defence*, (Brussels, Belgium, 2009).

[7] I. Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, The Guardian, May 17th (London, United Kingdom, 2007).