DR. ZSOLT HAIG

THE INFORMATION INFRASTRUCTURES OF THE INFORMATION SOCIETY[1]

AZ INFORMÁCIÓS TÁRSADALOM INFORMÁCIÓS INFRASTRUKTÚRÁI

This article introduces the evolution of the information infrastructures. It categorizes, classifies the information infrastructures that allow the existence and working of the information societies. It defines the information infrastructures and it emphasizes the risks of attacking these. Keywords: information society, information infrastructure, critical information infrastructure, infocommunications system

Az írás bemutatja az információs infrastruktúrák kialakulását. Kategorizálja az információs társadalom működését lehetővé tévő információs infrastruktúrákat. Meghatározza a kritikus információs infrastruktúrákat és hangsúlyozza azok támadásának veszélyességét. Kulcsszavak: információs társadalom, információs infrastruktúra, kritikus információs infrastruktúra, infokommunikációs rendszerek

Introduction

The information society is a very well developed and effective, but at the same time fairly vulnerable social and economic system. The basic element of this society is the information itself. Its quantity and quality is crucial for its users. According to this fact there is a harsh battle for its purchase, its safe storage and its effective appropriation. The possession of the right amount and proper quality of information can significantly assist to enlarge the economic benefit, to disclaim the incidental damages, as well as to create superiority against the other participant in a competition or conflict situation.

[1]The paper has been supported by the Bolyai János Research Scholarship of the Hungarian Academy of Science.

In our present time the information infrastructures producing, storing, processing and transmitting information, and of course the information itself assures the functioning of the social, political, economic, defence and cultural life. From this aspect these infrastructures are of accentuated importance, it is vital to constantly sustain their operability in the life of the society. Thus, the generality of them qualify as a critical infrastructure.

1. Characterization of the Information Society

The information society is a new type of social formation which is the descendant of the industrial society. The evolution of the information society has been induced by the apace development of electronics and computer engineering. The crescent influence of infocommunications technologies and networks can be equally noticed on the different fields of the individual, society, economy and culture. These technologies and networks offer a mellow selection of instruments and services, they have an influence on the behaviour and functioning of the individual, the society, the economy and the culture, they modify the forms of working, study and amusement. The subject of the information society, its leading spirit is not the material and the energy. It is the information. [1]

Due to the fact that information and knowledge have become determining, results in an intense and continuous utilization of scientific achievements. This is the reason why the present day society is called knowledge society.

The infocommunications networks modify the social connections. Our modern, speeded up life style, mellows or even dissolve those former familiar social communities just as families, residential, place of work and professional fellowships. The new technology and its supplies however create new communities that basically come to existence and work on a network principal. The infocommunications networks become more and more the new tool of connection, and people and groups form increasingly on a networked principal. [1]

The information society is an economic system built on a global, parliamentary democracy with a curb market with the information, knowledge and science in its focus which functioning is assured by informa-

tion networks. There are governmental, autonomous, administrative and defence institution systems operating built on broadband infocommunications networks, where public affairs, business and private matters can be dealt with on-line through information infrastructures from the distance. By the means of advanced infocommunications networks, on the fields of purchase, process, coming to a reasonable decision and transmitting it, this is the world's and history's fastest society. [2]

The infocommunications networks allow the state to function dependably and cheap. Through the infocommunications technology the connection between the individual and the state just as between the state and the non-governmental organizations progressively get a new foundation. Through the networks as well as the individuals and communities can directly take part in the local, regional and nationwide public affairs and making decisions. [3]

In the 90's Hungary recognized the possibilities hidden in establishing an information society and made the initial steps in order to fall into line with the level expected of the European Union. The most important stages of this process were the liberation of the telecommunication market, permission of broadband internet access in a wide range, and the elaboration of those strategies, that determine the policy of creating an information society.[2]

In the 2003 edition of Hungarian Information Society Strategy defines the following squarely: „With the generation of knowledge based economy and information society, the topmost common goal is to amend the life quality and life circumstances of the individuals and of the community and through this to create such a modern, European, Hungarian Republic in which everyone likes to live. In the 21st century this goal can be achieved doubtless and fastest along the national cultural and natural environment through the values of saving the knowledge output and knowledge propagation, economic competitiveness, fellowship, socially equal chances." [4:11.p]

At the same time it also notes that the biggest challenge is how to apply the well developed infocommunications technologies expansively through that the modernization of the economy and society, the

[2] National Information Society Strategy (2001); Hungarian Information Society Strategy (2003)

enlargement and closing up of their competitiveness becomes possible to close up with the leaders of the European knowledge societies. [4]

In the information society the government has to face new challenges:

— it has to support electric trade, online business activities, possibility and legitimacy of the electric management of the administrational matters;
— governmental and public affair supplies have to be accessible (e-governing, e- public affairs);
— people have to get prepared to be able to use infocommunications technologies and to use the supplies based on them. [3]

2. Categorization of the Information Infrastructure

As the different delivery, provider systems (e.g. traffic-, railway-, waterway- and energetic supply systems) are indispensable in the life of the society so it is necessary for the information society to have systems that forward, process, store information.

According to the definition of the Hungarian Declaratory Concise Dictionary "the infrastructure is an organization of elemental establishments, and organisations (flats, public works, trade, telecommunication, education, health care) that assures the undisturbance of the social and economic activities". [5]

The information infrastructures are the complexity of such stable or mobile facilities, tools, systems, networks respectively their supplies that allow the acquiring, generation, storage, dispensation and utilization of necessary information the information society needs for proper functioning. The elements information infrastructures are physical buildings and equipment, or else experts who can ran them professionally.

The secure operation of the information infrastructure permits of the organized, functional, professional and effective working of the society. The state of development, modernity, stage, quality of the supply, capable handling and last but not least the safety effect the information society's mechanism. [2]

Within the information infrastructure there are infrastructures heaps with different designation. According to utilization we differentiate them as follows:

— global information infrastructure;
— national information infrastructure and as a part of this,
— defence information infrastructure (figure 1.).

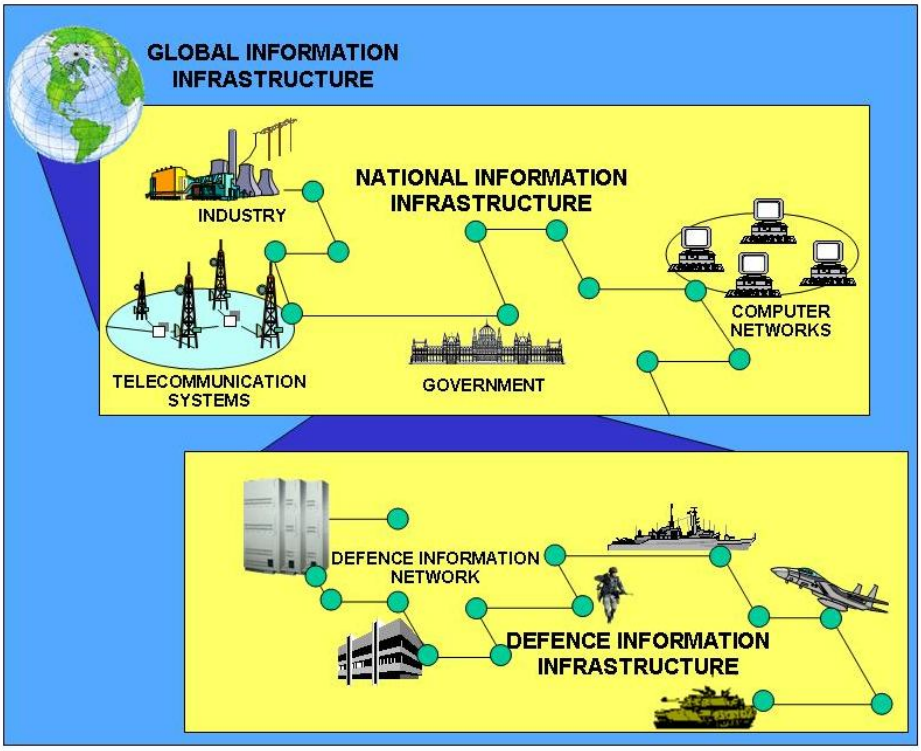

Figure 1.
Classification of the infrastructures according to utilization [2]

According to their functionality there are two groups of information infrastructures such as:

— functional information infrastructures and
— supportive information infrastructures. [2]

Further on we will introduce these two categories. With the dénouement of the information production period and the information society the created global economy is surrounded by the global information envi-

ronment. The technological basics of this global environment is that global information infrastructure, which is nothing else than all those wired and wireless telecommunication systems, computer networks, remote sensing systems, remote control systems, navigation systems and other infocommunications networks, that assure the global information gathering, storage, processing and transmitting. In this global information environment the internet gets more and more important since its supplies are resorted by the explosively growing electronic trade and electronic money market.

The country organisations connect to the world wide global information environment with the help of the national information infrastructures. This explains that the information infrastructure is a part of the global information infrastructure; its combination is after all a miniature reflection of that. The defence information infrastructures play a key role from a national security point of view. These defence information infrastructures cover all the instruments that transmit, process information of defence purpose, and instruments that store, handle and visualize information and data. The national defence infrastructure is of course a part of the national information infrastructure system beyond that it has an organic connection to the ally defence information systems. [2]

The designation of the functional information infrastructures is to physically enable the smooth, undisturbed working of some information functions of the society, namely to offer basic information supplies. Among the information infrastructures of the information society these have primacy. They guarantee the acquiring, generation, transmitting, processing and use of the information. The functional information infrastructures work in a big format, complex organized networks or systems. [2]

According to division to the information infrastructures we can count the following:

— telecommunication systems (analogue-, digital-, wired-, wireless-, cellular-, satellite telecommunications systems;
— broadcasting networks;
— management information systems (governmental-, administrational-, police-, military networks);
— air traffic control systems;

— navigation systems (autonomous navigation systems, Global Positioning System);
— remote sensing systems, remote control systems;
— robot control systems;
— computer networks.

Supportive information infrastructure is an overall definition of the research, developing and provider infrastructures. Their designation is to create and continuously assure all the necessary intellectual and financial basics and supportive background that are needed for the undisturbed functioning and developing of the functional information infrastructure that behoves the elemental information supply. [6]

Usually we count the following to the provider information infrastructures:

— electric power supply system;
— electronic, computer science and computer developing facilities;
— electronic and computer science companies;
— storehouses, wholesale supply companies.

3. Definition of the Critical Information Infrastructure

When we talk about the modern social appliance and its safe run, we have to emphasize the critical infrastructure from a national point of view because its proper functioning is crucial for the society. Insofar as they — as a consequence of any intervention or natural disaster — break down or become limited in their function — this fact could have unpredictable results on the national safety, the ability of economy and national defence. Therefore it is vital to be familiar with the critical infrastructures and their accurate boundaries since — through their systems — they lie under an infrastructure attack so thus they can become potential targets. [7]

In the past few years more than one example pointed out the vulnerability of the critical infrastructures and the necessity of their defence. It is enough to think of the diverse natural disasters (earthquakes, tsunamis) and terror acts (World Trade Center, Train bomb attack in Madrid, subway explosion in London). For the sake of materializing the defence

some countries and international organizations worked out their concept concerning this matter[3]. Examining and analyzing all the definitions and their divisions of the critical infrastructures and critical information infrastructures in the USA or in the well developed European countries it can be laid down as a fact that they correlate with each other. On this field as well Hungary started to fall into line with the EU. The 2112/2004 (V.7.) government regulation about the tasks of the fight against terrorism and the 2046/2007 (III.19.) government regulation about its modification already deals with the question of the defence of the critical infrastructures. The concreter regulation has been created in 2008 respecting the Green Book of the EU, when the government issued the 2080/2008 (VI.30.) government regulation about the National Programme for the Protection of Critical Infrastructures. The first appendix of the regulation (Green Book) takes the detailed bearings of the critical infrastructure definition, the sectors and tasks of the defence.

According to the Green Book „the critical infrastructures are such a network of connected, interactive elements, facilities or establishments, supplies, systems and procedures that bilaterally depend on each other, that are crucial regarding the functioning of the country (population, economy and government) and have a substantive role in maintaining a socially expected minimal level of legal certainty, public security, national security, economical capability, common health care and natural state.

As critical infrastructures are qualified those networks, recourses, supplies, products, physical or information technology systems, equipments, devices and all parts of the above, because the breakdown, destruction of the critical infrastructures or their functioning, them being out of order can have a direct or indirect effect temporarily or in the long run on the economic, social prosperity of the citizens, on the common health, common security, national security, on the working of national economy and government." [8: 220.p] The Green Book differen-

[3] e.g.: The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (USA). Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005. COM(2005) 576 final. Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight Against Terrorism, Brussels, 20.10.2004 COM(2004) 702 final. A strategy for a Secure Information Society – „Dialogue, Partnership and Empowerment". Brussels 31.5.2006. COM(2006) 251 final

tiates 10 sectors and 43 subsectors of the critical infrastructures[4]. Seeing through the sectors and subsectors it can be laid down as a fact, that our national Green Book are mostly conform with the EU regulation, it uses a similar definition of the critical infrastructures concerning this matter. [9]

In the last period of time the various infrastructures were a good target of different type and level of attacks. Until these attacks realized only in the physical dimension the country borders were somewhat of defence for them. The infocommunications systems getting global changed this relatively settled situation in fact very much. Nowadays even limited resources are able to plan and implement attacks against our critical infrastructures based on infocommunications systems. Asymmetric threats of different personal activists, unauthorized users and terrorists partly expanded, partly replaced the well known military threats. [10] Considering this we can say that the border line between the threats with military and civic nature fades more and more.

Though the 2080/2008 (VI.30) government regulation does not deal with the question of the critical information infrastructures, the threats out of the information dimension still make it reasonable to define and explain it. In the information society the critical infrastructures are not conform to the critical information infrastructures. According to the Green Paper on a European Programme for Critical Infrastructure Protection, the definition of the critical information infrastructures is: "ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)". [9: 19.p]

As you can see from this formulation, this document makes a difference between the two infrastructure categories. Earlier, the critical infrastructures of a country were as well as physically and logically separate, they did not depend on each other much. As the result of the developing information technology, nowadays these systems get more and more automated and they have a tight connection. [11]

Almost all kinds of critical infrastructures are controlled by different levelled and allocated infocommunications systems. Thus we can name with reason the country's infrastructure based on infocommunications

[4] Detailed listing in 2080/2008. (VI.30.) government regulation about the National Programme for the Protection of Critical Infrastructures

technology as the nervous system of the society and the result of this information infrastructures and their parts, too can be defined as critical infrastructures. According to this statement for example the public mobile telecommunication infrastructures — as critical infrastructures themselves — are also qualified as critical information infrastructures, or rather the system operator infocommunications networks of electric power supply systems. According to the definition of critical infrastructures sectors in the already mentioned Hungarian Green Book and the definition of the critical information infrastructures of the EU we can define and interpret our national critical information infrastructures based on the following:

— system operator infocommunications networks of electric power supply systems,
— infocommunications networks;
— infocommunications networks of traffic control and organization;
— infocommunications networks of water supply control;
— infocommunications networks of the food supply control;
— infocommunications networks of health care system;
— infocommunications networks of the monetary-economic system;
— infocommunications networks controlling industry production;
— infocommunications networks of governmental and self-government sphere;
— infocommunications networks of the defence sphere.

Although the real targets of the attacks that intend to disturb the smooth functioning of the society are the critical infrastructures — because they are the basic of its working — but the information based attacks and threats against them effect the infocommunications systems with different levels and importance. These systems became the strategic targets of threats because the attacker can induce major damages with a small investment in power and appliances.

Conclusions

The well developed, networked infocommunications systems create the basic of the infocommunications society's evolution. The technological and social conditions of this up to date social formation have been cre-

ated in Hungary as well. Since the 90's the actual government has been committed to the establishment of the Hungarian information society.

The information infrastructures give the basics to the information society's working and development. This is the reason why the majorities of these infrastructures are crucial in the life of the society and can be qualified as critical information infrastructures.

The tight connection among the critical information infrastructures, the interdependency among them significantly increases the vulnerability of the information society. The more integrated, the more complex they are, the more extended is the connection between them, the more they depend on each others functioning, the higher degree they are exposed to the new type of threats, thus is the pressure higher to realize the defence and security.

References

1. Dr. Haig Zsolt, Dr. Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. 286 p. ISBN: 963-327-391-9
2. Horváth Pál: Gondolkodjunk el magunkról és a világról. HTE hírlevél, 2008. No. 10. 1-3p.
3. Horváth Pál: Gondolkodjunk el magunkról és a világról. HTE hírlevél 2008. No. 11. 1-4p.
4. Magyar Információs Társadalom Stratégia. Informatikai és Hírközlési Minisztérium. November, 2003.
5. Magyar Értelmező Kéziszótár, MTA, Budapest, 2002.
6. Haig Zsolt–Kovács László–Makkay Imre–Seebauer Imre–Vass Sándor–Ványa László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002.
7. Várhegyi István, Makkay Imre: Információs korszak, információs háború, biztonságkultúra. Budapest, 2000. OMIKK
8. 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. Határozatok tára No. 31. Budapest, 30. June 2008. 217-231p.
9. Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final.
10. Gerencsér András: Rövid összefoglalás kritikus információs infrastruktúrák védelméről. http://www.isaca.hu/addons/news_ 1626_CIIP_GerencserAndras.pdf (downloaded: 27. 05.2009.)
11. Dr. Munk Sándor Információs színtér, információs környezet, információs infrastruktúra. Nemzetvédelmi Egyetemi Közlemények, 2002. No. 2. ZMNE, Budapest, 133-154.p. ISSN 1417-7323