HADMÉRNÖK

IV. Évfolyam 3. szám - 2009. szeptember

Kovács László
kovacs.laszlo@zmne.hu

POSSIBLE METHODOLOGY FOR PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES

Abstract/Absztrakt

The main objective of this paper is to examine the methodology for protection of critical information infrastructure in EU and Hungary. Western countries heavily depend on these infrastructures. However, we can not see any certain steps toward the identification and protection of these systems. Without these steps we can not state: there has been taken all necessary measures on the field of critical infrastructure and critical information infrastructure protection.

Jelen írás fő célja megvizsgálni az Európai Unió és a hazai kritikus információs infrastruktúrák védelmének lehetséges módszerét. A nyugati országok nagymértékben függenek ezektől az infrastruktúráktól. Ennek ellenére sem ezek azonosítása, sem ezek védelme érdekében nem látni azt az előrelépést, amely alapján kijelenthetjük: kritikus infrastruktúráink és kritikus információs infrastruktúráink védelme érdekében megtettünk minden szükséges intézkedést.

Keywords/kulcsszavak: *critical information infrastructure, protection, CIIP ~ kritikus információs infrastruktúrák, védelem, KIIV*

INTRODUCTION

In our age one of the most important factors is the information. There are many infrastructures that provide the social, political, economic, security and cultural life operations by production, storage, processing and transmitting information. These systems and assets are the information infrastructures.

Many of them are critical because they are essential part of our everyday life. Their lack or even failure could cause enormous human and financial damages. In addition, traditional critical infrastructure systems including energy (gas or electric power), transportation, water utilities, food distribution, public health, and finance and banking systems also include information infrastructures. All critical infrastructures are increasingly dependent on information and communication. These also could be critical for our society.

The potential natural disasters or terrorist attacks, which threaten the critical infrastructure and critical information infrastructure as well, are dramatically increasing today.

In addition in last years, blackouts in North America and some part of Europe are massive evidence of serious vulnerabilities of our critical infrastructures and critical information infrastructures.

However, the protection of critical information infrastructure and mainly their methodology for identification have been applied in many countries with a serious challenge. There are many unanswered questions yet: What is the most critical among the information infrastructures? How can we identification and prioritize them?

In the following parts this study tries to give answers for some of these questions.

CRITICAL INFRASTRUCURES AND CRITICAL INFORMATION INFRASTRUCTURES

Over the last few year number of studies concerned with critical infrastructures[1] and the critical information infrastructures protection (ie: [1], [2], [3], [4], [5]).

However, it is necessary to give an overview on them as a basis for the further examinations.

In 1997, the Report of the President's Commission on Critical Infrastructure Protection defined the infrastructure as „*more than just a collection of individual companies engaged in related activities; it means a network of independent, mostly privately-owned, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services."* [6]

Critical infrastructure is a term to describe assets and systems that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for the following:

- electricity production, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (drinking water, waste water/sewage);
- agriculture, food production and distribution;
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbors, inland shipping);
- financial services (banking, clearing);
- emergency services (disaster relief);
- security services (police, military).

According to the European Union issued Green Paper on a European Programme for Critical Infrastructure Protection the critical infrastructure *"can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. To save the lives and property of people at risk in the EU from terrorism, natural disasters and accidents, any disruptions or manipulations of CI should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States (MS), their citizens and the European Union. The recent terrorist attacks in Madrid and London have highlighted the risk of terrorist attacks against European infrastructure. The EU's response must be swift, coordinated and efficient."* [7]

[1] Critical infrastructures were originally considered to be those whose prolonged disruptions could cause significant military and economic dislocation. [8]

This Green Paper has set up an indicative list of critical infrastructure sectors which is shown in Table 1.

Table 1. Indicative list of critical infrastructure sectors [7]

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

Hungarian governmental decision called *National Program on Critical Infrastructure Protection* also set up a list of critical infrastructure that is shown in the next table:

Table 2. Critical infrastructure sectors and subsectors in Hungary [9]

Sector	Subsector	Responsible
I. Energy	1. oil production, refinery, storage and distribution 2. gas production, storage, transport and control system, distribution 3. power generation, transmission and control system, distribution	Ministry of Transport, Telecommunication and Energy
II. Infocommunication technology	4. information systems and networks 5. SCADA 6. internet 7. wired and mobile communication 8. radio telecommunication and navigation 9. satellite telecommunication and navigation 10. broadcasting 11. postal services 12. governmental computer and electronic services	Prime Minister's Office Electronic Government Center, Ministry of Transport, Telecommunication and Energy
III. Transportation	13. road transport 14. rail transport 15. aviation 16. waterborne transport 17. logistics centers	Ministry of Transport, Telecommunication and Energy
IV. Water	18. potable water service 19. surface and groundwater quality monitoring 20. sanitation and cleaning 21. water protection 22. flood protection, dams	Ministry of Environment and Water
V. Food	23. food production 24. food safety	Ministry of Agriculture and Rural Development
VI. Health care	25. hospital care 26. emergency control 27. health reserves and blood 28. high security biological laboratories 29. health insurance	Ministry of Health
VII. Finance	30. payment and securities accounting infrastructure and systems 31. bank and credit security	Ministry of Finance
VIII. Industry	32. chemical production, storage and processing 33. transport of dangerous goods, 34. hazardous waste treatment and storage, 35. nuclear materials production, storage, processing 36. nuclear research 37. military production 38. vaccines and pharmaceuticals	Ministry of Transport, Telecommunication and Energy, Ministry of Defence, Ministry of Local Government, Ministry of Justice and Law Enforcement, Ministry of National Development and Economy
IX. Law and governance	39. government facilities, equipment 40. administrative services 41. justice	Ministry of Local Government, Ministry of Justice and Law Enforcement, Ministry of Defence,
X. Public security	42. defense installations, devices, networks 43. enforcement infrastructures	Ministry of Justice and Law Enforcement, Ministry of Local Government, Ministry of Defense

However, it is necessary to make difference between critical infrastructures and critical information infrastructures. According to the European Green Paper Critical Information Infrastructures (CII) are: *„ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).”* [7]

Previous studies already have been classified the Hungarian critical information infrastructures several times. These classifications based on the professional competence, methodology or approach to reflect of the test teams.

The first classification based on information system, mainly computer networks. According to that CII are the following:

- command and control computer networks of power (energy) systems;
- communication systems (wired, mobile, satellite);
- command and control computer networks of transport;
- computer networks of finance and banking;
- computer networks and early warning- and communication systems of defense and security;
- computer networks of health care;
- governmental computer networks. [4] [10]

The other classification based on both computer networks and further infocommunication systems. According to that CII are the following:

- ICT systems and computer networks;
- Supervisory Control And Data Acquisition
- internet and internet infrastructure;
- wired communication services;
- mobile communication services;
- radio telecommunication and navigation;
- satellite telecommunication;
- broadcasting;
- administrative information technology and communications;
- vital communication systems of critical infrastructures. [3]

Although the two divisions used different basis to the examinations, but a lot of similarities and a lot of overlap are included.

METHODOLOGY OF PROTECTION

Lessons learned from international policies and practices show that protection of critical information infrastructures build up different phases. The next figure shows these – sometimes – parallel phases:

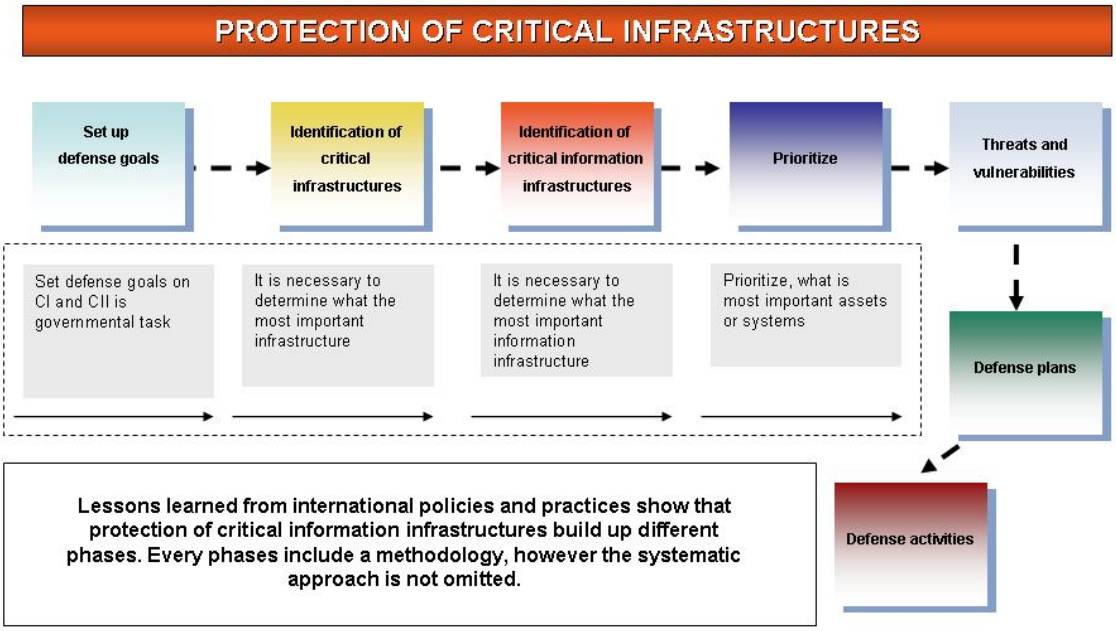

Figure 1. Phases of Critical Infrastructure Protection

These phases are:

1. define defense policy;
2. methodology of critical infrastructures identification;
3. methodology of critical information infrastructures identification based on critical infrastructure identification, and the methodology of interdependency identification;
4. prioritize;
5. methodology of threats and vulnerabilities identification;
6. methodology of working out the ideal protection and action plans;
7. comparison and analysis of ideal protection plan and the real situation of protection.

Other noticeable approach is in the United States National Infrastructure Protection Plan (NIPP) which is shown in Figure 2.

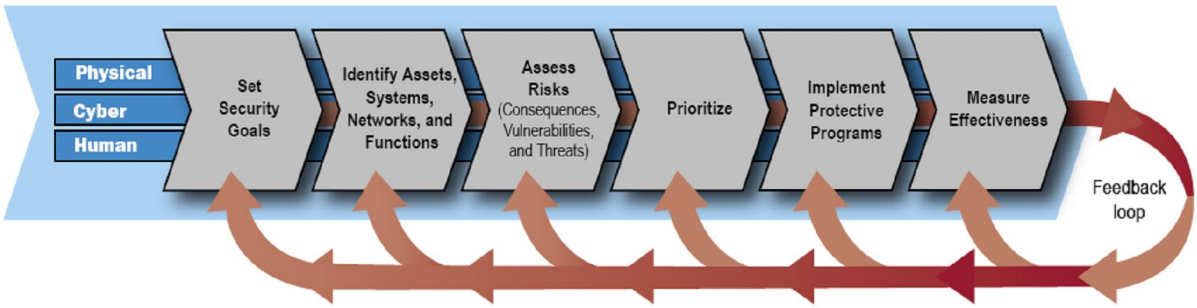

Figure 2. NIPP Risk Management Framework [11]

The systematic approach is necessary during the working out of methodology, since only in this case is provided to take into account the full spectrum of defense. Figure 3. illustrates the main components of the systematic approach.

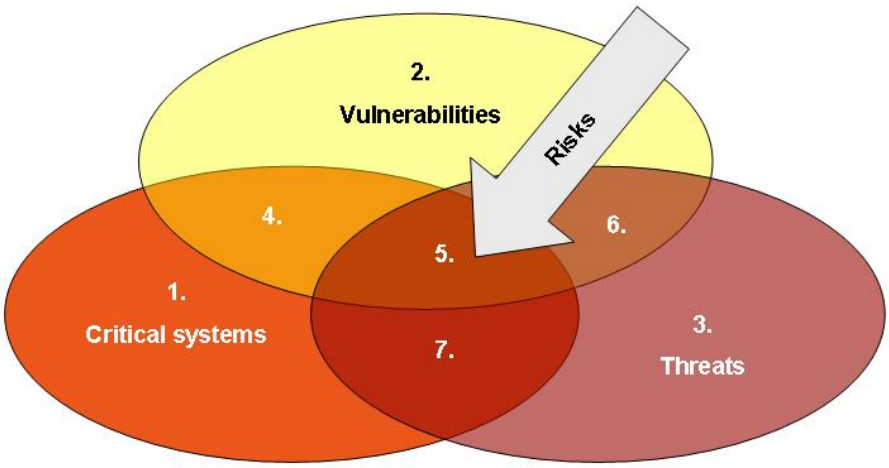

Figure 3. Main elements of systematic approach [12]

These elements are the following:

1. critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat exposure;
2. vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat exposure;
3. threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information);
4. critical assets for which there are known vulnerabilities, but no known threat exposure;
5. critical assets for which there are known vulnerabilities and threat exposure;
6. threat has acquired specific knowledge and/or capability to exploit vulnerability although not a critical asset vulnerability;
7. critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat. [12]

Based on these facts this paper shortly examines the phases of the critical infrastructure and critical information infrastructures protection.

Phase 1: Define defense policy

The main goals of defense already have been defined in Hungary. There are some government decisions and related laws on defense:

- National Security Strategy of Hungary (2073/2004. (IV. 15.) government decision);
- Government decision on actual tasks against terrorism 2112/2004. (V.7): it prescribed to joint the EU's European Programme for CIP - EPCIP;
- Hungarian Disaster Recovery Law (LXXIV. 1999);
- Hungarian "Green Paper" 2080/2008. (VI.30.): National Critical Infrastructure Protection Program, which is decisive progress in the field of security objectives.

The Hungarian Green Paper has defined some important tasks for the Government:

- the national coordinating body and the functions are defined as: in terms of efficiency and consistency are necessary to set up a national coordinating body (for example, Prime Minister's office), which bring together, manage and promote the sector and the government and the various owners of critical infrastructure protection responsibilities;

- the designation of coordinating the critical sectors;
- propose to the European level of critical infrastructure elements designation. [9]

Analyzing the Green Paper from the critical information infrastructure point of view, it is clear that the document does not define the domestic tasks on the field of national critical information infrastructure protection; it has been mean only as a part of the critical infrastructure protection.

This is supported by the fact that the government classified among the critical infrastructure threats "*the economic or political motives, critical information systems and networks against abuse and cyber-attacks (cyber-terrorism, DDOS attacks, and incidents of mass phising)"* [9]

On this basis, the national critical information infrastructure protection policy required the following the governmental functions:

- it is necessary to define the concept and the definition of critical national information infrastructure;
- it must be to identify those elements which are critical information infrastructures of critical infrastructures;
- must be explore the specific threats to critical information infrastructures;
- to be designed and organized specific simulations for information infrastructure, which can be basis to explore the vital key elements of the economy, society and the government;
- must be defined and should be mapped the direct and indirect effects to each other of domestic information infrastructure and critical infrastructure;
- to be determined the impacts of national information infrastructure to the neighboring countries[2];
- the government coordinating body functions must be supplemented with the critical information infrastructure owners and operators, and representatives of the national CERT-s;
- it is necessary to examine whether the domestic information and communication infrastructure, and the early warning system, and the management of emergency communications are fit for a possible terrorist attack;
- it is necessary to give more effective training for the conscious and secure Internet and ICT use. [1]

Phase 2: Methodology of critical infrastructures identification

There was mentioned above classification of critical infrastructure (Table 1 and Table 2).

Work of critical infrastructures identification starts with a simple categorization. The infrastructure should be listed into one of mentioned subsectors. After that the next step is further categorization by coverage, impact and duration effect. This could be:

- **coverage:** international, national, regional, territorial or local;
- **impact:** no impact, minimal, temperate or significant. Beside these factors the following impacts also could be considered:
  - population impact (number of casualties, disease, serious injuries, etc.)
  - economic impact (impact on GDP, significant economic losses, and / or production, the progressive deterioration of services);
  - environmental impact (impact on population and the their living environment);
  - interdependence (the other elements of critical infrastructure);

[2] The European Council directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection also defines this task. [13]

- political impact (loss of public confidence).

- **duration effect**: how long does a serious impact on loss of infrastructure (immediately, less than 24-48 hours, a week, longer duration).

The following criteria are shown in Table 3 also could help in the identification.

Table 3. Criteria for critical infrastructures. [8]

Infrastructure	Criteria for Being Considered Critical. Vital to			
	national defense	economic security	public health and safety	national morale
telecommunications information networks	x	x		
energy	x	x		
banking/finance		x		
transportation	x	x		
water			x	
emergency services			x	
government			x	
health services			x	
national defense	x			
foreign intelligence	x			
law enforcement			x	
foreign affairs	x			
nuclear facilities, in addition to power plants			x	
special events				x
food/agriculture			x	
manufacturing		x		
chemical			x	
defense industry	x			
postal/shipping			x	
national monuments icons				x

Phase 3: Methodology of critical information infrastructures identification based on critical infrastructure identification, and the methodology of interdependency identification

The next task is identifying the critical information infrastructures based on the critical infrastructures. It is important to note that interdependency and intradependency are necessary to examine continuously.

The above mentioned categorizations could help in the work of CII identification:

- command and control computer networks of power (energy) systems;
- communication systems (wired, mobile, satellite);
- command and control computer networks of transport;
- computer networks of finance and banking;
- computer networks and early warning- and communication systems of defense and security;
- computer networks of health care;
- governmental computer networks. [4] [10]

The other classification based on both computer networks and further infocommunication systems. According to that CII are the following:

- ICT systems and computer networks;
- Supervisory Control And Data Acquisition
- internet and internet infrastructure;
- wired communication services;
- mobile communication services;
- radio telecommunication and navigation;
- satellite telecommunication;
- broadcasting;
- administrative information technology and communications;
- vital communication systems of critical infrastructures. [3]

Phase 4: Prioritize

The prioritization is one of the most challenges in the protection of critical assets. The following factors could mean some assistance in this task: [3]

1. critical facilities;
2. injuries can affect the functioning of a number of another infrastructures;
3. interdependency;
4. geographical location;
5. ownership.

Phase 5: Methodology of threats and vulnerabilities identification

The identification of threats and vulnerabilities must include the following:

- to explore the system(s), duties, functions;
- to explore the development and operation of the system in order to determine the possible failures;
- to identify the weaknesses of critical systems;
- where possible, to determine the duration of any failure (the different periods of time may affect the system or other systems which are interdependent);
- to develop recommendations to reduce the vulnerability and possible dependencies.

The following chart (Figure 4.) shows the possible methodology of the risks and vulnerabilities exploration.

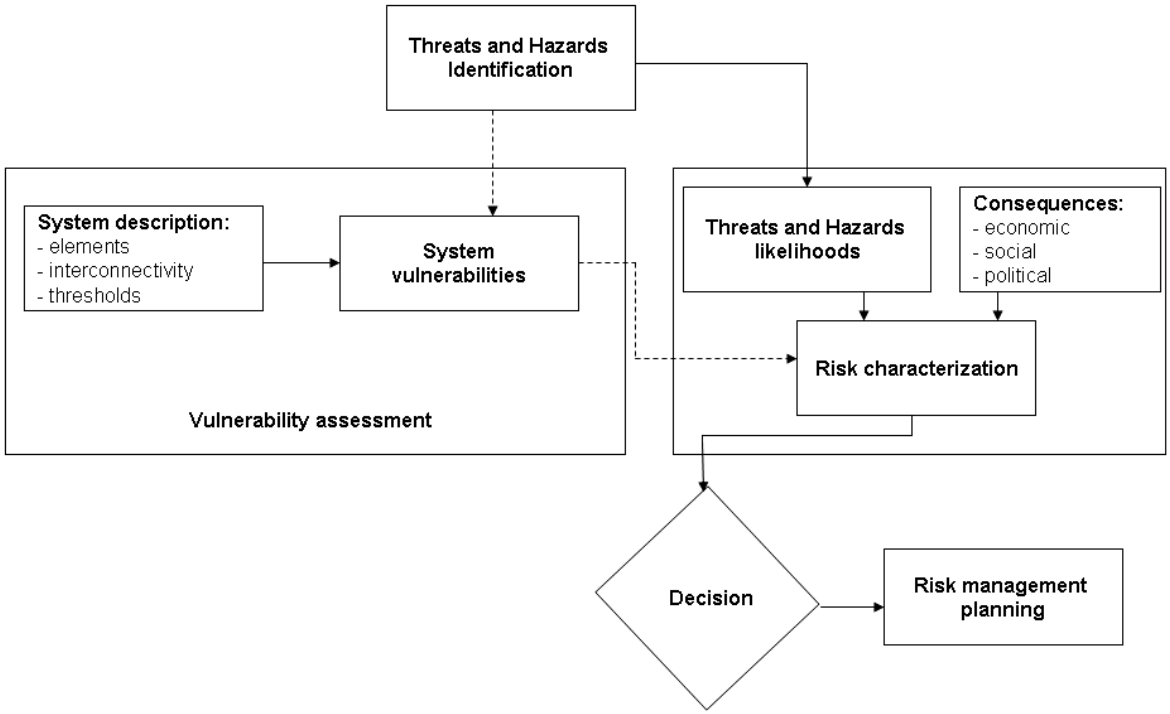

Figure 4. Vulnerability assessment methodology [14]

Phase 6: Methodology of working out the ideal protection and action plans

This study's objectives is not included the development of ideal security solutions and security solutions.

However, it is important to indicate this fact, since this phase is an integral part of the critical infrastructure and critical information infrastructure protection activities.

Phase 7: Comparison and analysis of ideal protection plan and the real situation of protection

This study's objectives is not included the comparison and analysis of ideal protection plan and the real protection activities.

However, it is important to indicate this fact, since this phase is an integral part of the critical infrastructure and critical information infrastructure protection actions.

STEPS TOWARD THE REAL PROTECTION AS CONCLUSIONS

In summary, based on the facts mentioned above, many additional tasks are required for European and national critical infrastructure and critical information infrastructure protection.

The possible steps are the following:

- a consistent methodology to determine the critical infrastructures and the critical information infrastructure;
- develop a unified procedure for determining vulnerabilities;

- develop a unified risk assessment methodology (or adaptation) and application of the common principles;
- create a common warning and alert system to national and European level;
- create a critical information infrastructure protection "manual" based on unified guidelines;
- establish a principles-based common European education and training system.

REFERENCES

[1] Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai. HADMÉRNÖK on-line tudományos lap, 2008. június, ISSN 1788-1919 http://www.zmne.hu/hadmernok/2008_2_kovacsl.php (2009.08.10.)

[2] Précsényi Zoltán–Solymosi József: Úton az európai kritikus infrast-ruktúrák azonosítása és hatékony védelme felé. Hadmérnök, 2007. március ISSN 1788-1919. http://zrinyi.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html (2009.08.10.)

[3] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori értekezés. ZMNE, Budapest, 2007.

[4] Kovács László: Kritikus információs infrastruktúrák, Egyetemi jegyzet. ZMNE, 2007.

[5] Mógor Judit - Földi László - Solymosi József: Lépéseka kritikus infrastruktúra védelmének magyarországi szabályozása felé. HADMÉRNÖK on-line tudományos lap, 2008. december, ISSN 1788-1919 http://www.hadmernok.hu/archivum/2008/4/2008_4_mogor.pdf (2009.08.10.)

[6] Critical Foundations Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, Wa-shington, 1997. október

[7] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final.

[8] John Moteff, Claudia Copeland, and John Fischer Resources, Science, and Industry Division: Critical Infrastructures: What Makes an Infrastructure Critical? Report for Congress. Congressional Research Service - The Library of Congress. Updated January 29, 2003

[9] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[10] Haig Zsolt – Kovács László – Ványa László: Kritikus információs infrastruktúrák támadása, védelme. Dunaújvárosi Főiskola Közleményei, XXIX/1. ISSN 1586-8567

[11] National Infrastructure Protection Plan. US Department of Homeland Security. Washington DC, 2006. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (2009.08.10.)

[12] DoD Critical Infrastructure Protection NDIA Information Briefing. July 3, 2002. http://www.dtic.mil/ndia/2002security/bozek.pdf (2009.08.10.)

[13] European Council directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection (9403/08).]

[14] George H. Baker: A Vulnerability Assessment Methodology for Critical Infrastructure Facilities.
http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=george_h_baker (2009.08.10.)