AARMS Vol. 14, No. 3 (2015) 331–342.

The Role and Security of Money from the Aspect of Cyber Warfare

CSER Orsolya[1]

Security is one of the most basic human needs, which never appears alone, but always in response to an emergency situation. Internal security of a state means the protection of the political, social and economic order, and the elimination of hazards, such as the instrument of economic terrorism, cyber attack.

Cyberspace is a major arena of modern warfare. Attacks against it have made it important for banking systems that IT systems be developed in the most secure manner both inside and outside the organisation.

Keywords: *cyber-attack, financial security, IT system, critical infrastructure, IT operations, electronic service, bank security*

Security

Security is one of the most basic human needs, which never appears alone, but always in response to an emergency situation. [1] The danger of an attack against Hungary and its allies implemented by conventional weapons currently is minimal. Internal security of a state means the protection of the political, social and economic order, and the elimination of hazards, such as the instrument of economic terrorism, the cyber attack. [2]

For security, the uninterrupted operation of the economy and the assurance of the conditions for development are basic prerequisites, whose economic aspects are:

- *assurance of economic stability*: efficient economic structure, secure international trade relations, free competition;
- *establishing stable financial conditions*: moderate inflation, manageable debts and loans, stimulating interest system.

Financial security means the stability of the budget of the organisations belonging to the defence sector. Accordingly the government of Hungary is committed to supporting the budget of the Ministry of Defence in the 2013–2015 budgetary years at least in the nominal value of the scheduled budgetary contribution for 2012 in the Government Resolution 1046/2012 (II. 29.) [3] ensuring the budget sources to create defence expenditure and the conditions of long-term planning.

Hungary's defence expenditures to the proportion of the GDP – 0.65% in 2014 – are largely behind the expenditures spent for this purpose by NATO member countries (2.0% based on the NATO recommendation). In accordance with the Government Resolution 1046/2012 (II. 29.) the planned defence expenditure for 2014 is 0.655% of GDP, for 2015 0.6%. [3] Starting from the 2016 budgetary year there will be at least a 0.1 percentage point annual increase

1 e-mail: cserorsi77@gmail.com

in GDP proportion until the amount of aid by 2022 – approaches the average of the NATO member states – reaching 1.39% of GDP. The planning of the budget quotas is available for the defence sector in accordance with this.

The main aim of the all-time expenditure target of the Ministry of Defence is to be able to defend Hungary's independence – with the cooperation of the alliance – with our country's volunteer army, filled up with professional personnel. Besides this, resulting from our NATO and European Union membership, performing international roles and fulfilling alliance obligations by participating in operations carried out by the UN and the Organization for Security Co-operation in Europe[2] (OSCE) to become capable of contributing to the strengthening of international security; and to fulfil the tasks resulting from the defence preparation.

The custody service at financial institutions is a closely related field to the topic of financial crises and their management. The conceptual structure and approach of the defence and war economy sciences can be implemented on a seemingly distant field like the banking community, which acts in defence of our values. [4]

One of the methods of economic terrorism is cyber attacks. It is an important question, since the aim is first and foremost managing financial crisis's and related bank tasks. Bank security is of critical importance, since a bank system may be targeted by a cyber attack in given cases. Thus it is necessary that an adequately secure environment should be assured in regard to banks, therefore security must be built into the IT systems. The reasons for the occurrence of exceptional events can be deliberate or careless behaviour, for example a cyber attack against an IT system, or the totality of unexpected events, for example a natural disaster. As a consequence of the given event, life and property security is seriously endangered, hindering or paralysing the normal operation of the bank. To anticipate and prevent these exceptional events, and to decrease the measure of the disadvantage that occurred, tight cooperation must be developed with local military and police organizations.

It is expected by the state, the actors of the economy and also civilians that these basic vital or critical infrastructures operate with the highest security possible. [5] For the defence of infrastructure elements against terror activities, natural disasters, and accidents it is important that disturbance or manipulation of the operation of the infrastructures should be avertable and preventable, and as fast, exceptionally and manageably as possible.

National Security Strategy (NSS)

The concept of security is gaining a more and more expansive interpretation. In the continuously changing security environment these days, the challenges, risk factors and threats have already emerged – individual, society, states and regions, and global level – at several levels, and affect a wide range of individuals, government and non-governmental organizations, and transnational actors. By now it has become necessary to treat the political, military, economic and financial, social (within this human and minority law) and environmental dimensions of security together.

Based on evaluating the assets and interests, and analysing the security environment Hungary's National Security Strategy defines those national targets, tasks and expansive governmental tools, with which the EU and NATO member Hungary vindicates its national secu-

2 peacekeeping operations

rity interests in the international political and security system of the 21st century. [6] Those security elements which are present in case of a financial crisis – for example cyber attack against the bank system of the country – are important aspects of ending the emergency. The aim of the NSS is to provide direction for the government and the private sector in questions of security policy and including financial issues. Because of this, in its philosophy it follows an expansive and all governmental approach. The security of the country is a public affair, therefore one of the tasks of the strategy is to give a usable guideline in everyday life besides the professional circles in Hungarian security policy thinking.

The NSS defines all those factors that determine financial security in the operation of the economy of each nation state:

- cash supply – in case of bank crisis limitation of cash supply;
- instant deposit withdrawal panic – for example the Postabank scandal (February 1997);
- financial reserve – in the case of crisis situations;
- financial moratorium – limitation of money withdrawal from financial institutions.

The 30th article of the NSS in 2012 is about financial security, giving a guideline to the government sector for managing and solving the problems of financial crises (for example cyber attack). [7]

To prevent and manage the conflicts of our age requires a global and expansive approach. Sustainable security and stability requires the expansive approach, aligned with each alternative usage of the crisis management methods – including development policy methods – the integrated civilian and military approach and the capability development, and strengthening the cooperation of international actors. The expansive approach must be implemented on a national government level as well.

The national security strategy can only be successful and efficient in case of an all-government approach, participation and responsibility, making the institutional frames meet the challenges and allocating adequate resources. The global financial and economic crisis gives an unprecedented challenge for the whole North Atlantic community. The long-drawn-out and deep crisis weakens the security institute system of the developed countries, among them, Hungary's, and the cohesion of the international organisations and co-operational frameworks, and decreases the resources that can be spent on strengthening security. All of this requires the innovative and more efficient concentration of the resources we have to strengthen our security skills. In this field, organizational cooperation continues strengthening, and the importance of the conscious usage of the possibilities hidden in multinational cooperation. According to the 5th article of the North Atlantic treaty, collective defence is the cornerstone of Hungary's security. The active contribution to collective defence and security is the most important security political obligation of Hungary. The Strategic Conception of NATO sets those directions with which the alliance – adapting to the changed security environment – is capable of fulfilling its role as set in the North Atlantic Treaty (Washington Treaty) and assuring the defence of its member countries. Terrorism remains the significant global threat of our age that emerges in different forms in time and space, continuously changing, and endangering our alliance system and our common values. Hungary's terror threat is low, yet at the same time terror threats of foreign origin or against Hungarian interests abroad must be considered. Besides this, foreign terror activities may have security and economic consequences affecting our country.

Critical Infrastructures (CI)

Modern societies largely depend on technical and virtual infrastructure systems (energy supply, drinking water supply, IT networks, etc.) whose complex system is characterised by their dependency on each other. Therefore, increasing the security of infrastructures became a primary concern in the security policy of the developed countries. The disruptions to the operations of these systems, and the temporary outage or destruction of certain elements have significant impacts on our daily lives, the efficient operation of the economy and the government.

According to the general definition, critical or vital infrastructures are "facilities or elements of such systems that are necessary to fulfil essential functions of society – thus assuring especially health, personal and property security of civilians, economic and social public services – and the outage of which due to the lack of continuous fulfilment of these tasks would cause consequences." [8]

These infrastructures are partially owned by the state, partially by the private sphere, and are operated by both of them. Critical infrastructures may be damaged, dysfunction may occur in their functioning, or they may even be destroyed as a result of terror attack, national disaster, negligence, accident, computer hacker activity, crime and/or misconduct. The main areas for increasing the security of the infrastructures are putting the defence of individuals and societies, and the security of critical infrastructures on a higher level. In all three fields, the dangers and threats may have physical or IT origins, or may be caused by the complexity of the systems. The solution requires investigating the physical, IT and psychological level reasons of the new threats and risks, understanding their relationship/context, and managing them.

On the whole the CI are:

- those networks, resources, services, products, physical or IT systems, equipment, tools and the elements of that equipment;
- whose failure, disturbance, outage or destruction of operation;
- directly or indirectly, temporarily or long term may have a serious impact;
- to the economic and, social wellbeing of citizens, public health, public security, national security, the national economy and the operation of the government.

Based on the definition of national critical system elements in Annex 2 of the Act CLXVI of 2012 [8] on the identification, designation and protection of critical infrastructures, finance can be considered a critical infrastructure sector.

Table 1. The sub-sectors of financial critical infrastructure. [8]

	A	B
	Sector	*Sub-sector*
17	finance	commercial, payment, and clearing and cash accounting infrastructures and systems of financial instruments
18		bank and credit institution security
19		cash supply

The CI extend to several economic sectors, among others banking and finance, transportation and distribution, the energy industry, the system of public utilities, health care, food supply, information, and indispensable state services. Some of the critical elements of these sectors do not strictly belong to the concept of "infrastructure", but in fact they are such networks or supply chains, which support the assurance of some basic product or service.

The possibility of catastrophic terror attacks threatening critical infrastructures is ever increasing. The results against the industrial control systems of the critical infrastructures can be very different. One of the types of catastrophic failure of the infrastructures is when the failure of one part of the infrastructure leads to the failure of the rest, causing a domino effect. This type of failure may occur as a consequence of a synergic effect of the infrastructural sectors effect on each other. A simple example of this can be an attack against the energy providing public utility, if the energy supply stops other electrical devices – such as banks systems as well – may stop. The sequence of events following each other also may cause serious damage, and through the public utilities may result in the outage of bank and financial systems. For the sake of the defence of critical infrastructures against terror activities, national disasters, and accidents, it is important that the disturbance or manipulation of the operation of infrastructures should be avertable and preventable, and as fast, exceptionally and manageably as possible. Therefore increasing the security of infrastructures became a primary concern in the security policy of developed countries. The solution requires investigating the physical, IT and psychological reasons for the new threats and risks, understanding their relationship, and managing them.

Cyber Defence

Cyberspace is a major arena of modern warfare. [9] Attacks against it have made it important in the case of financial and banking systems that the IT systems should be developed in the most secure manner with the coordinated use of hardware, software and or hardware. Based on this, cyber defence aims to maintain accessibility to information and information based processes in its own network IT systems, and to ensure the efficient usage of these systems equally in peace, crisis or conflict. Cyber warfare means network warfare materializing in the IT dimension. To put it simply, it is an activity to influence the confidentiality, integrity, and availability of critical IT structures using IT physical and human tools. The demands of detecting cyber attacks require tight cooperation and organised action between the developers, producers, distributors, administrators, users of the IT systems and the service provider, legislative and intelligence service organizations. [10] The operational speed of the attackers of IT systems may exceed the recognition and response skills, including human solutions. For the sake of efficient cyber defence it is primarily important to estimate the seriousness of the event (damage to the system, compromising, malware penetrating the system) by automated methods, and reduce the negative effects of those. The detection of attacks in time is a basic prerequisite of starting the recovery and taking the necessary countermeasures.

The threats that can be implemented in information warfare can be divided into four categories: "compromising, deceiving, interruption of service, physical destruction." [11] All four categories mean risk to those independent or networked weapons and support systems (bank systems), which largely depend on IT systems. The threat may originate from organised powers (states) or unstructured belligerents (hackers).

Compromising can have different forms, for example the unauthorized acquisition of technology or software failure, unauthorised penetration of the system, use of malware, collection of data by intelligence services, or a psychological operation. To protect the automated IT systems, in the first step the threats against them must be understood, for example compromising the data and information, partial or complete hindrance, damage to services. The best tool for countering this is training and tight cooperation between the operators and the users. As a preliminary examination, minimal information must be collected, probable disciplinary proceedings must be indicated, and a proposal for further investigation should be submitted. Assessing the damages after being compromised must be done by a centrally controlled system that consists of a central database and targeted developed programmes and projects. The security monitoring of IT systems is interception, reading, copying or recording of own official telecommunication, whose purpose is to provide material for analysis that enables the precise definition of the security level of the automated bank IT systems. In this IT environment, IT operations mean coordinated activity in the physical, IT and knowledge dimensions which are capable of influencing belligerents by affecting their information, information based processes and information communication systems. The aim of IT operations is gaining information superiority, power and eventually leadership superiority.

The primary threats of IT operations are: compromising, damage to data, or breaking of an IT operation. In case of security problems, prevention, fast response, and minimising the damage can be considered a major task. In all of these tasks, the widespread usage of IT solutions appears with more and more emphasis. The diversity of the definition based on different approaches proves the necessity of cooperation for the sake of the defence of IT operations, risk related defence tasks, and training extended to all details.

It is widely accepted that a successful cyber attack would cause only a few casualties even in the worst case, but in regard to critical infrastructure services it may result in losses. For example, due to a successful cyber attack against a bank network, customers would miss the bank services until the experts successfully fix and restore the network.

The risk of attack through cyber space – by IT or other methods – in the case of the banks made it important that IT systems should be developed in the most secure way possible, inside and outside the organisation. [12]

The financial systems have a very important role, since without their adequate operation a part or the whole of the financial processes would become unserviceable, or at least significantly hindered.

The Security of the Financial System

The macroeconomic cycle must continuously operate so that the perpetuity of the cash supply, and by that real flows (production) may be assured. The protection against fake money and money forgery – in its physical form – means the importance of the protection and security of money.

Financial service activities can be initiated and continued only in case of the existence of information and control systems to reduce operational risks, and a plan to manage emergency situations. To achieve this, it would be worthwhile to develop a practical scheme for the future – by the Best Practices (Best Practises) method already used in several fields – by which the financial authorities (banking sector) are capable of a coordinated and immediate

response to counteract attacks against them, and to anticipate and prevent exceptional events, and to decrease the measure of the disadvantage that occurred, tight cooperation must be developed with the local military and police organizations.

In case of the security of a bank system (bank security) the most important criteria are the following: [13]

- Financial service activities can be initiated and continued only in case of the existence of information and control systems to reduce operational risks, and a plan to manage emergency situations.
- The financial institution must develop a regulation system in relation to the security of its IT system used to fulfil its financial, auxiliary financial service activities, and must ensure the defence of the IT system to the ratio of the risks.
- In the regulation system, IT demands, the plan for the assessment and management of the security risk of the usage in the fields of planning, acquisition, operation and control must be covered.
- Based on evaluation of the result of the risk analysis, in proportion with the security risk there must be provided at least management procedures ensuring the self-defence of the IT system, closeness to its critical elements, control ensuring comprehensiveness, and also a security environment which logs the events of critical processes in terms of the operation of the IT system, and is capable of the systematic (possibly automatic) and substantive evaluation of this logging, and offers the capability of managing irregular events.
- To fulfil its activity, to keep its records up-to-date and secure, the financial institution must implement the defence measurements justified by the security risk analysis, and must meet the following minimum requirements:
  - the IT system needed to provide the services, and auxiliary equipment to ensure the perpetuity of services, and in the case of non-availability of this equipment other solutions replacing them – ensuring the perpetuity of the activities and services;
  - such security backups and back up rend (type and method of the backups, backup and restore tests, rules of procedure) of the software elements of the IT system that enables the possibility of restoring the system within the critical restoration time of the service. These backups must be stored separately in a fireproof way for risk aspects, and, and must provide defence of the same level with the source system access of the backups;
  - a plan to manage the exceptional events hindering the perpetuity of its services.

Consequently, bank security activity is institutional thinking of all those planning, organisational, managing, executive and controlling conditions, which serve the defence of their own objects, assets of the financial institution, and the security of employees and customers.

For managing exceptional events, the following can be defined:

- In proportion with the size, the character, order of magnitude, complexity of the financial, auxiliary financial service activity of the finance institute must have a reliable management system, and is obligated to apply efficient procedures to identify measure, manage, track and report the emerging risks within its framework.
- Besides this, it must have written regulations of procedure, rules to measure, manage the operational risk, and emergency and conduct of business continuity plan to maintain continuous operation, and to decrease the resultant damage caused by serious interruption of the conduct of business.

The security of the financial system is continuously threatened, for example catastrophes and war situations, and the activities of fraud and robbers. This is a potential attack against critical infrastructures, in this case against the banking sector, where an adequately safe environment must be ensured and security must be built in the IT systems. High level management must be prepared against these problems, (NATO Crisis Management Exercise [CMX] exercises), and then acting together to stop the threat and restore the safe conditions, where the Hungarian crisis management system decision preparation and decision making procedures and the cooperation with the NATO headquarter and the member countries is practiced.

NATO Crisis Management Exercise

Our critical infrastructures are vulnerable and attackable. The experts cannot see any definite steps which would strengthen the adequate, complex defence of these networks –especially the bank and financial computer networks. All of that means that critical infrastructures are extremely vulnerable. The countries with advanced military and IT culture consider the defence of critical IT structures one of the most serious challenges of the beginning of the 21st century.

So far no such study has been made of a "Digitális Mohács" in Hungary, one that would take into account what chain reactions may be caused by an expansive sequence of activities including IT attacks relating to the critical IT systems, for example a cyber attack against our bank system – as was simulated in November 2012 during the CMX 2012 drill. One attack targeting the IT structures may cause operational malfunctions lasting for days in the country.

The main aim of the NATO CMX crisis management and cyber defence (attack against the bank system) drill was to make consensus decisions needed for united action against the challenges of our age: [14]

- enforcing the 5th article of the NATO treaty – the member countries acted together to prevent the attack and to restore the systems;
- practicing the decision preparation and decision making processes of the Hungarian crisis management system, and cooperation with the NATO headquarter and the member countries;
- for the CMX exercise the cyber attack in Estonia in 2007 served as an example (these days there are no "real" wars without cyber attacks).

The experts drew attention to the fact that, in case of these types of attacks, one must primarily aim for prevention, since it is almost impossible to prepare for attacks planned and targeted by other organisations. Consequently, bank security activity is institutional knowledge of all those planning, organisational, management, executive and controlling conditions, which serve the defence of its own objects, the assets of the financial institution, and the security of employees and customers. The crisis concentrates the impact of the events, intensifying the reactions of people living in a country or the members of a nation. [15] The attention concentrates on the organisation in crisis, whose change is inevitable. In this case the majority of a country can be affected by the national (nationwide) crisis simulated in the article if the events planned by the terrorists occur. The period before the crisis can be called the stage of foreboding signs, when the warning signs multiply. It is quite often possible to determine that turning point after which the crisis is already inevitable.

The basic fields of crisis management are the following:

- *preventive*: prediction and evasive averting, prevention;
- *active*: prevention and repression of the growing and spreading of the threats - based on the imminent crisis's predicted by the appreciable signs;
- *reactive*: strategy and measures to eliminate the occurring crisis, i.e. crisis management policy.

Problem management can be divided into parts, which are the following:

- *diagnosis*: recognition of the failure and success factors;
- *assessment of the situation* ;
- *therapy*: operative actions to extinguish the problematic anomaly.

In case the counter steps are not efficient, the chronic stage comes, where the crisis broadens, serious damage occurs, and there is a very little chance of the solution. It is exactly to prevent this that the NATO CMX exercises are planned every year, when through simulation realistic situations are created, which may cause crisis situations. The bank security, which may be targeted by cyber attack in a given situation is an important aspect, hereby it is necessary that, in the case of banks, an adequately safe environment be ensured. Towards this, security should be built into IT systems. The reasons for the occurrence of exceptional events can be deliberate or careless behaviour, for example a cyber attack against an IT system, or the totality of unexpected events, for example a natural disaster. As a consequence of a given event, life and property security is seriously endangered, thus hindering, or paralysing the normal operation of the bank. To anticipate and prevent the exceptional events, and to decrease the measure of the disadvantage that occurred, tight cooperation must be developed with the local military and police organizations.

National Response System

The Estonian critical IT infrastructures [16] were attacked on the 27th April, 2007, by an external Distributed Denial of Service (DDoS) attack that was supplemented with spamming, and defacing. The main targets were the computers of the Estonian Parliament, and the banks, ministries, newspapers and electronic media. The attack hit both Estonia and NATO unprepared, although its implantation required few resources.

In Hungary, so far, no incident caused by external attack has come to light, but in 2009, several IT errors occurred that blocked the operation of the given IT infrastructure. [17] This caused difficulties to tens or hundreds of thousands of people; it was widely covered in the media, and caused significant prestige loss for the operating institution.

Therefore Hungary also has its share of bitter experience in connection with the outage of IT systems, but the impact of direct, organised attacks for the time being is unthinkable.

In the operation of financial systems, in bank transactions, electronic services have an increasingly emphasised role in Hungary. The secure operation of these services is a critical question from a national security aspect, since without those the economic and financial functioning of the country would confront serious obstacles.

The legislature is trying to guarantee the security of these services by law, but in certain areas currently there are no standard technical recommendations which would determine the requirements of security, integrity and availability. [18: 192–194] [18: 414–417] Internation-

al trends and domestic experiences both show that electronic bank services are permanent targets of organised crime, hackers, and official organisations of other countries.

To provide a perfect defence would mean disproportionately high costs, however based on the principle of expectable carefulness it is necessary to securely develop the publicly accessible services. That means that security thinking must be present already at the planning of the new applications. For bank services it is possible to develop security solutions on several levels. The security level of banks can be significantly increased, and thus the rising national security risk can be considerably decreased. The relationship between crisis management and the exceptional rule of law can be an important factor in ensuring that the solution of arising problems would be executable. After the events of Tallinn the crisis is nothing else than an emergency situation whose solution requires the coordinated action of several government organisations and local governments following the lead of the Estonian Government's crisis management committee. All of these means a serious threat to the security and cannot be managed with conventional tools.

Today in Hungary there is no standardised crisis management system, and creating it is not a realistic objective. In the Government Decree 278/2011 (XII. 20.) about the destination, duties, regulations of procedures, the obligations of the participants of the National Response System, in accordance with the NATO Crisis Response System [20] the demand for it was formulated earlier. The existing crisis management subsystems and the skills connected to them are divided by departmental segments; their cooperation often follows an ad hoc style.

Nevertheless the aligned implementation of the civil and military law enforcement skills is necessary, because of the conformity with the NATO Crisis Response System as well. [19] As a result of this, an expansive approach is necessary, which gives a complex answer to the complex challenges, implements aligned skills, extinguishes the duplicates, and forms cohesion in civilian and military law enforcement cooperation.

Summary – Suggestions

To perform financial service activities an information and control system to reduce operational risks and a plan to manage emergency situations is needed.

Based on the evaluation of the result of the risk analysis, in proportion with the security risk there must be provided at least management, procedures ensuring the self-defence of the IT system, closeness of its critical elements, control ensuring comprehensiveness, and also a security environment which logs the events of the critical processes in terms of the operation of the IT system,

Towards this, it would be worthwhile to develop a practical scheme for the future – by the Best Practices (Best Practises) method already used in several fields – by which the financial authorities (banking sector) are capable of coordinated and immediate response to counteract the attacks against them.

Nevertheless, examining the defence sector, for the armed organizations the stability of the budget has an extreme importance, by which planning predictability can be ensured for the future, and the capability development and the task based planning.

Financial service activities can be initiated and continued only in case of the existence of information and control systems to reduce operational risks, and a plan to manage emergency situations.

To achieve this, it would be worthwhile to develop a practical scheme for the future – by the Best Practices (Best Practises) method already used in several fields – by which the financial authorities (banking sector) are capable of coordinated and immediate response to counteract the attacks against them.

References

[1] GAZDAG F., TÁLAS P.: A biztonság fogalmának határairól. *Nemzet és Biztonság*, 1 1 (2008), 3–9.

[2] GAZDAG F. (szerk.): *Biztonsági tanulmányok – biztonságpolitika*. Budapest: ZMNE, 2011.

[3] 1046/2012. (II. 29.) Korm. határozat a honvédelmi kiadások és a hosszú távú tervezés feltételeinek megteremtését szolgáló költségvetési források biztosításáról. *Magyar Közlöny*, 24 (2012).

[4] CSER O.: *Értékmegőrzés válság idején a pénzintézeteknél*. http://193.224.76.4/download/konyvtar/digitgy/publikacio/cser_orsolya01.pdf (downloaded: 20 02 2015)

[5] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. *Magyar Közlöny*, 47 (2013).

[6] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. *Magyar Közlöny*, 19 (2012).

[7] BESENYŐ J.: Újfajta háború? Internetes hadviselés Grúziában. *Sereg Szemle*, VI 3 (2008), 61–63.

[8] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. *Magyar Közlöny*, 154 (2012).

[9] HAIG Zs., VÁRHEGYI I.: A cybertér és cyberhadviselés értelmezése. *Hadtudomány*, XVIII (2008), 1–12.

[10] TOMOLYA J., PADÁNYI J.: A terrorizmus jelentette kihívások. *Hadtudomány*, 3–4 (2012), 34–67.

[11] HAIG Zs., KOVÁCS L., MUNK S., VÁNYA L.: *Az infokommunikációs technológia hatása a hadtudományokra*. Budapest: NKE, 2013.

[12] KOVÁCS L., ILLÉS Zs.: Cyberhadviselés. *Hadtudomány*, 1–2 (2011), 29–41.

[13] CSER O.: Biztonságunk egyik záloga a hatékony civil-katonai együttműködés. *Hadtudomány*, 3–4 (2013), 104–116.

[14] *A NATO kibervédelmi gyakorlatán is jól vizsgáztunk. (CMX 12 NATO Válságkezelési gyakorlat nemzeti feladatai.)* http://bitport.hu/biztonsag/a-nato-kibervedelmi-gyakorlatan-is-jol-vizsgaztunk (downloaded: 21 02 2015)

[15] KISS P.: A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében. *Hadtudomány*, 3–4 (2012), 68–79.

[16] HAIG Zs., KOVÁCS L.: Fenyegetések a cybertérből. *Nemzet és Biztonság*, 5 (2008), 61–69. www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (downloaded: 01 03 2015)

[17] KOVÁCS L., KRASZNAY Cs.: Digitális Mohács – kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság*, 1 (2010), 44–56. www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf (downloaded: 28 02 2015)

[18] VÍGVÁRI A.: *Pénzügy(rendszer)tan*. Budapest: Akadémiai Kiadó, 2009.

[19] KESZELY L.: *A válság és a különleges jogrend kapcsolata, különös tekintettel a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszerre.* www.hadijog.hu/wp-content/uploads/2014/03/Keszely-V%C3%A1ls%C3%A1greag%C3%A1l%C3%A1s.pdf (downloaded: 25 02 2015)

[20] 278/2011. (XII. 20.) Korm. rendelet a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről. *Magyar Közlöny*, 155 (2011).