AARMS Vol. 19, No. 1 (2020) 83–93.

10.32565/aarms.2020.1.7

Governmental Regulation of Cybersecurity in the EU and Hungary after 2000[1]

Tamás SZÁDECZKY[2]

The term information security evolved to cybersecurity nowadays, which emphasises the interdependence of information assets and the importance of cyber-physical systems. Parallel to this, the need for appropriate management of the EU and government strategies and new public administration tasks also appeared.

In the European Union, the first measure concerning this issue was the establishment of the European Union Agency for Network and Information Security (ENISA) in 2004, mostly with consultative tasks. The first official cybersecurity strategy in the EU, called the Open, Safe and Secure Cyberspace, was accepted in 2013. Afterwards, ENISA's role has been strengthened as well as its range of tasks were broadened. Beside the critical infrastructure protection efforts, the Network Information Security (NIS) directive and related legislation were a giant leap towards a common level of cybersecurity in the community. The formation of an EU Cybersecurity Act and filling NIS with more practical guidance is an ongoing process nowadays.

Despite being a post-socialist country, Hungary is in the first line of legislation on cybersecurity in the community. Since 2005 there were several government decrees, from 2009 the first act-level rules on the information security of some governmental services. Based on the National Security Strategy, the National Cybersecurity Strategy was formed in 2013. The same year the first information security act applicable to all government, local government, governmental data processing and critical infrastructure service providers has come into force. The alignment of the National Cybersecurity Strategy to NIS directive happens these days.

Thus, the regulation of cybersecurity in the EU and in Hungary are heading in the right direction, but the practical implementation today is far away from the strategic objectives. The community is lagging far behind the United States of America and China, just to mention the most important players in the field.

Keywords: *cyber strategy, information security legislation, incident response, ENISA.*

[1] Supported by the ÚNKP-17-4-III-NKE-26 New National Excellence Program of the Ministry of Human Capacities.

[2] Ph.D., associate professor, National University of Public Service, Faculty of Public Governance and International Studies, Department of Public Management and Information Technology; e-mail: szadeczky.tamas@uni-nke.hu; ORCID: https://orcid.org/0000-0001-7191-4924

Introduction

The word cybersecurity seems to be a bit overused nowadays, but as other researchers have already demonstrated, it is different from the "classical" term information security. In both terms, information-based assets stored or transmitted using information and communication technologies (ICT) are included. But information security also includes paper-based information. According to the definition of the International Telecommunication Union's (ITU) definition in 2008, cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, the organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity—which may include authenticity and nonrepudiation—and confidentiality. This is pretty much similar to the term information security. However, the term cybersecurity includes non-information-based assets (e.g., a high-voltage substation) that are vulnerable to threats via ICT. This is similar to the interdependency between critical infrastructure elements. Thus, "in cyber security the assets that need to be protected can range from the person him/herself to common household appliances, to the interests of society at large, including critical national infrastructure". [1: 100] The new model of cybersecurity needs a different approach to security organisation: the classical security models have to be revised. [2]

The importance of cybersecurity is well-known and often communicated by decision makers. However, the implementation and preparedness have deficiencies. This might happen because of lack of knowledge, resources or experience.

Table 1. *Legal regulations about cybersecurity in the EU and Hungary.*
[Edited by the author.]

Year	The European Union	Hungary
2004	Regulation on establishing ENISA	
2012		National Security Strategy
2013	EU Cybersecurity Strategy The new regulation on ENISA	National Cybersecurity Strategy, Information Security Act
2016	NIS directive	
2017		
2018		
2019	Cybersecurity Act	
2020		The new National Security Strategy

Technological development, as I have already pointed out, made local system security improvements indispensable. [3] In case of e-government systems, a higher level of the problem also exists: attack against multiple systems or against a full infrastructure. This

can be part of a conventional war, as cyberwar, or may be an unconventional event, called cyberterrorist attack; they all concern cybersecurity. Thus, a major part of cybersecurity can be only managed on governmental or supranational level, with cybersecurity strategies, legal regulation, and dedicated authorities. [4] Table 1 shows parallelly the changes in the EU and Hungary, which will be detailed in this article.

Cybersecurity Strategy in the EU

Before forming any exact strategy, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10th March 2004 establishing the European Network and Information Security Agency* [5] came into force. The regulation established ENISA, with the following objectives (Article 2):

- "the Agency shall enhance the capability of the Community, the member states and, as a consequence, the business community to prevent, address and respond to network and information security problems;
- the Agency shall provide assistance and deliver advice to the Commission and the member states on issues related to network and information security falling within its competencies as set out in this Regulation;
- building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors;
- the Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security."

It is important to remark the verbs used: enhance, provide, develop, and update. They show us an intention to form a soft agency without policy-making power. The exact plans with ENISA were also unclear. [6]

The tasks aligned with the objectives above were the followings:

- collect appropriate information to analyse current and emerging risks;
- provide advice to stakeholders;
- enhance cooperation between different actors;
- facilitate cooperation between the Commission and the member states;
- contribute to raise awareness;
- assist the Commission and the member states in their dialogue with industry;
- track the development of standards;
- advise the Commission on research;
- promote risk assessment activities;
- contribute to Community efforts to cooperate with third countries;
- express its own conclusions independently.

As we see from the list above, the tasks are supportive functions. There are no regulatory, standardisation or audit functions dedicated to ENISA. In contrast, in the field of data protection, the European Data Protection Supervisor has authority to audit EU organisations.

The bodies of ENISA are the Management Board, the Executive Director, and the Permanent Stakeholders' Group.

The first official cybersecurity strategy in the European Union was formed with the *JOIN (2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union*. It's the *Open, Safe and Secure Cyberspace* formed on 7th February 2013. It states that "the borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent." [7] The first statement is: "The EU's core values apply as much in the digital as in the physical world, the same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain." [8] According to *Tallinn Manual 2.0*, most of the physical world international law rules can be applied on the cyberspace conflicts, but there are some unregulated issues. For those new points, additional rules are required. But cybercrimes are typically a field where all real-life legislation can be used, only the context, the device and the methodology changed.

The strategy defined five strategic priorities, which address the challenges:

- "achieving cyber resilience;
- drastically reducing cybercrime;
- developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- develop the industrial and technological resources for cybersecurity;
- establish a coherent international cyberspace policy for the European Union and promote core EU values." [7]

In the first strategic priority—achieving cyber resilience—the need to modernise and strengthen ENISA was articulated. [9]

After nine years of ENISA's operation and providing nearly 300 publications—with focus topics incident and risk management, critical infrastructure protection, trust services and computing cloud—a new regulation came into force. *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21st May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004* has changed the objectives: [Section I. Article 2. para 1–5]

- "the Agency shall develop and maintain a high level of expertise;
- the Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security;
- the Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market;
- the Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents;

- the Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors." [10]

The tasks were also changed according to the objectives (Article 3):

- "support the development of Union policy and law, by advising, providing preparatory work, and analysing;
- support capability building by supporting the member states, promoting voluntary cooperation, assisting by the operation of a Computer Emergency Response Team (CERT);
- support the raising of the level of capabilities of national/governmental and Union CERTs promoting dialogue and exchange of information, with a view to ensure that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices;
- support voluntary cooperation;
- cooperate with Union institutions, bodies, offices and agencies;
- contribute to the Union's efforts to cooperate with third countries and international organisations." [10]

The most important change in the tasks was the establishment of CERT–EU, as a new service, and also a part of Computer Security Incident Response Teams (CSIRT) network according to Network Information Security (NIS) directive *(Directive [EU] 2016/1148)* Article 12. Para. 2. Incident management became more important in the operation of ENISA with these changes than in 2004. The incident management theory and practice are very wide; they range from operational procedures to governmental response. Illustrative key topics are ISO/IEC 27035, ITIL-based incident response, forensics, and operation of CSIRTs. [11]

The only change in the organisation was the staff's addition under the Executive Director, and the Management Board shall establish an Executive Board.

In 2016, the European Commission adopted the *Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final*. The document dealt with the making of most of NIS cooperation mechanisms and enhancing the capabilities and responsibilities of ENISA. The section also mentions European Cybercrime Centre (EC3) at Europol as a possible cooperation partner. The Commission is required to evaluate ENISA by 20 June 2018, but plans to do it earlier.

So a future change was foreseeable with the *2017/0225 (COD) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and the repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").* The voting was forecasted to June 2018. Furthermore, on 13th September 2017, the President of the European Commission, Jean-Claude Juncker announced an implementation toolkit for the Network and Information Security Directive; and a report to ensure an effective response in case of cyber-attacks in the member states.

As the topic is in the focus of general interest and even had many political debates, the acceptance lasted for a while. The new act is *Regulation (EU) 2019/881 of the European*

Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). [12]

The objectives of ENISA changed slightly:

- the Agency shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks;
- the Agency shall assist the Union institutions, agencies, and bodies, as well as the member states, in developing and implementing policies related to cybersecurity;
- the Agency shall support capacity building and preparedness across the Union, by assisting the Union, member states and public and private stakeholders in order to increase the protection of their network and information systems, develop skills and competencies in the field of cybersecurity, and achieve cyber resilience;
- the Agency shall promote cooperation and coordination at Union level among the member states, Union institutions, agencies and bodies, and relevant stakeholders, including the private sector, on matters related to cybersecurity;
- the Agency shall increase cybersecurity capabilities at Union level in order to complement the action of member states in preventing and responding to cyber threats, notably in the event of cross-border incidents;
- the Agency shall promote the use of certification, including contribution to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthen trust in the digital internal market;
- the Agency shall promote a high level of awareness of citizens and businesses on issues related to the cybersecurity.

The tasks improved heavily: the task list consists of 60 elements, grouped into the following seven articles:

- Tasks relating to the development and implementation of Union policy and law;
- Tasks relating to capacity building;
- Tasks relating to operational cooperation at Union level;
- Tasks relating to the market, cybersecurity certification, and standardisation;
- Tasks relating to knowledge, information and awareness raising;
- Tasks relating to research and innovation;
- Tasks relating to international cooperation.

Another focus is the forming of new European cybersecurity certification schemes (see Article 46): “The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes.” [12] Those schemes,

with the additional national schemes defined in Article 57, may provide a higher level of IT security interchangeability within the EU.

Cybersecurity Organisation in Hungary

The first comprehensive security and defence policy system of Hungary after the political change in 1989 did not recognise cyber threats. Neither the *National Assembly resolution no. 94/1998 (XII. 29.) on the security- and defence policy principles of the Republic of Hungary*, nor the *Government Decision 2073/2004. (IV. 15.) on the National Security Strategy of the Republic of Hungary*, nor the *Government Decision 1009/2009. (I. 30.) on the National Military Strategy of the Republic of Hungary* included cyber defence as an objective. According to these policies and strategies, the defence against cyber-attacks was treated individually, even in the legal regulation.

The first regulations in Hungary dealing with information security of governmental organisations were the following:

- *Government Decree 195/2005 (IX. 22) on security, interoperability and uniform use of electronic administration systems;*
- *Government Decree 84/2007 (IV. 25) on security requirements of the Central Electronic Service System and related systems;*
- *Government Decree 193/2005 (IX. 22) on detailed rules for the electronic filing;*
- *Government Decree 194/2005 (IX. 22) on requirements for electronic signatures and the associated certificates used in the administrative proceedings, as well as requirements for certification service providers issuing the certificates;*
- *Government Decree 182/2007 (VII. 10) on the regulation of the central electronic service provider system.*

The *Act on Electronic Public Service* (accepted in 2009) was the first act-level regulation dealing with information security in governmental organizations. [13]

In sum, we may say that a relatively low awareness of the legislator and the business was observable in the usage of international IT security standards, despite its significance and the high risk in some areas. [14] No obligations were found in acts of the Hungarian Parliament for enforcement of standards in IT security. There have been built-in self-control procedures in some acts, but in practice, those procedures actually did not work efficiently. [15]

In 2009 a small change was commenced with the adoption of *Act LX of 2009 on electronic public services*. It has highlighted the requirement of security as a basic principle.

According to *Act LX of 2009 on electronic public services*, organisations providing ICT based public services ensure the publicity of data of public interest (according to the Act on data protection and freedom of information) and protection of personal and any other data during the provision of services. [16]

IT security-related requirements were detailed in the following regulations:

- *Government Decree 223/2009 (X. 14) on the security of electronic public services;*

- *Government Decree 224/2009 (X. 14) on the central electronic system service's recipient identification and authentication services;*
- *Government Decree 225/2009 (X. 14) on electronic public services and their use;*
- *Government Decree 78/2010 (III. 25) on requirements of electronic signatures in administration and certain rules for electronic communication.*

A major change in the regulation started with the *Government Decision 1035/2012 (II.21.) on Hungary's National Security Strategy*, which stated that the information security of electronic public services, critical infrastructure and cyber defence capabilities have to be improved. The next step in this way was the *Government Decision 1139/2013 (III. 21.) on Hungary's National Cybersecurity Strategy*, which is still in force. The main objectives of it are to stablish incident reporting and response capability, develop international cooperation, and develop trainings, exercises, baseline security and cooperation. These are actually very similar to the aims of the NIS, but articulated somewhat earlier.

The recent cyber operations increased the global political awareness in this area, thus on 25th April 2013 the Hungarian Parliament accepted *Act L of 2013 on the electronic security of state and local government organisations*. It's scope is slightly broader than just state and local government organisations, but also includes national data processors and critical infrastructure, therefore even private companies might be included (e.g. public utilities). [17] The act is based on international best practices and standards (e.g. ISO/IEC 27001:2013), although does not reference them directly. The law operates with the essential items known in the information security field as the CIA triad (confidentiality, integrity, and availability). The act requires the integrity and the availability of information systems in a closed, complete, consistent way, proportionate to the risks for the electronic system and components. It is important to explicitly include the proportionality of the security control implementation to risks. This enforces the conduction of a risk assessment and decisions based on that. This changes the malpractice of implementing security measures in an ad hoc manner, and is to minimise security budgets. [18]

The act established the National Electronic Information Security Authority under the control of the Ministry of National Development. The new task of vulnerability testing and log analysis was dedicated to the National Security Authority and the long before established Government Computer Emergency Response Team (GovCERT) was moved to the Special Service for National Security, which is a secret service in Hungary.

Afterwards the field of cybersecurity, including the organisations above, was handed over to the Ministry of Interior with *Government Decree 187/2015. (VII. 13.).* Thus, the National Cyber Defence Institute was formed in the Special Service for National Security with the following features:

- administration by National Electronic Information Security Authority;
- incident management and response by GovCERT-Hungary;
- forensic log analysis and vulnerability testing by National Security Authority.

Another change coming into force in the meanwhile was the NIS directive. The National Cybersecurity Strategy has to be aligned with the requirements of NIS, *Chapter II (National frameworks on the security of network and information systems) Article 7 (National strategy on the security of network and information systems).* This is an ongoing process right

now. Also, the *Information Security Act* is affected by NIS, *Article 8 (National competent authorities and single point of contact)* and *Article 9* (*Computer security incident response teams* [CSIRTs]). The National Cyber Defence Institute is planned to be a competent national authority according to Article 8 of *NIS Directive (EU) 2016/1148*. There are four designated CSIRTs according to Article 8 of this directive:

- LRLIBEK for critical infrastructures, operated by the National Directorate General for Disaster Management, Ministry of the Interior;
- MILCERT, operated by the Military National Security Service;
- Hun-CERT, the Hungarian Computer Emergency Response Team for Council of Internet Service Providers, operated by the Hungarian Academy of Sciences, Institute for Computer Science and Control;
- and NIIF-CSIRT, which is the Computer Security Incidents Response Team of NIIF/HUNGARNET, the Internet provider of universities, higher education institutes, some secondary schools, academical research organisations and non-profit institutions in Hungary, operated by the National Information Infrastructure Development Institute.

Conclusion

ENISA was established in 2004 as a consultative body. Both the EU and the Hungarian Cybersecurity Strategy was accepted in 2013. The strategies implied changes in the treatment of the field of cybersecurity at the higher level. The objectives and tasks of ENISA have been changed, and the Hungarian authority was formed that year. The next step was the NIS directive and its implementation in the member states' law, which also provides reinforcement to EU legislation to improve ENISA.

One of the main objectives and tasks both for ENISA and in the Hungarian regulation is the training. Even in the private sector, there is a huge need for well-trained IT personnel. The required level of training is much higher in the cybersecurity than in classical back-office processes. In order to provide hands on knowledge, also real-life laboratories shall be used for such training. [19]

Another field of cybersecurity is that of military or cyber warfare. Many EU members, including Hungary, is a NATO member, which shapes our defence politics to a greater extent than the EU Common Security and Defence Policy. NATO recognised cyberspace as a "Domain of Operations" at the Warsaw Summit in 8–9 July 2016. In fact, there are no elements which are directly applicable at the member state level. There are many potential threats, like PSYOPS in the social media. [20: 117] Also, Internet of Things (IoT) as a civilian technology may pose risks to the defence sector. [21] But the fact that cyberspace became the fifth domain of operation, and the requirement that all military operations shall include such operations, will have a positive effect on defence.

Several changes happened in the previous years in the European legislation, and therefore preparedness to cybersecurity risk is much better nowadays, but we lag behind the United States of America and behind China. [22] Thus there is a long way to go.

References

[1] SOLMS, R. – NIEKERK, J.: From information security to cyber security. *Computers & Security,* 38 (2013), 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004

[2] LEUPRECHT, C. – SKILLICORN, D. B. – TAIT, V. E.: Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly,* 33 2 (2016), 250–257. DOI: https://doi.org/10.1016/j.giq.2016.01.012

[3] SZÁDECZKY, T.: Risk Management of New Technologies. *Academic and Applied Research in Military and Public Management Science (AARMS),* 15 3 (2016), 279–290.

[4] *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10th March 2004 establishing the European Network and Information Security Agency.*

[5] LEWIS, J. A.: National Perceptions of Cyber Threats. *Strategic Analysis,* 38 4 (2014), 566–576. DOI: https://doi.org/10.1080/09700161.2014.918445

[6] HEARN, J.: Moving forward? *Security & Privacy,* 1 2 (2013), 70–71. DOI: https://doi.org/10.1109/MSECP.2003.1193215

[7] *JOIN (2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union.*

[8] *Tallinn Manual 2.0* https://www.cambridge.org/hu/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB (Downloaded. 14.09.2020)

[9] RUOHONEN, J. – HYRYNSALMI, S. – LEPPÄNEN, V.: An outlook on the institutional evolution of the European Union cyber security apparatus. *Government Information Quarterly,* 33 4 (2016), 746–756. DOI: https://doi.org/10.1016/j.giq.2016.10.003

[10] *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21st May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.*

[11] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

[12] TONDEL, I. A. – LINE, M. B. – JAATUN, M. G.: Information security incident management: Current practice as reported in the literature. *Computers & Security,* 45 9 (2014), 42–57. DOI: https://doi.org/10.1016/j.cose.2014.05.003

[13] DEDINSZKY F.: *Informatikai biztonsági elvárások.* [Information security requirements.] Budapest, MeH-EKK, 2008.

[14] SASVÁRI, P. – NEMESLAKI, A. – RAUCH, W.: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Public Management Science (AARMS),* 14 1 (2015), 63–78.

[15] SZÁDECZKY, T.: Information Security Law and Strategy in Hungary. *Academic and Applied Research in Military and Public Management Science (AARMS),* 14 4 (2015), 281–289.

[16] KISS, A. – SZŐKE, G. L.: New principles and instruments in the field of Data Protection Law. In RAPPAI, G. – FILÓ, Cs. eds.: *Well-being in Information Society 2014.* (Conference proceedings) Pécs, PTE, 2014. 208–215.

[17] MUHA L. – KRASZNAY Cs.: Kibervédelem Magyarországon: áldás vagy átok? [Cyber defence in Hungary: Bless or curse?] *HWSW*, Paper 50206, 2013. www.hwsw.hu/hirek/50206/kibervedelem-biztonsag-jog-torveny.html (Downloaded: 10.06.2020)

[18] SZABÓ, Zs. M.: Cybersecurity issues of pension payments. In. SZAKÁL, A. ed.: *IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017*. New York, IEEE, 2017. 289–292.

[19] DOMÍNGUEZ, M. – PRADA, M. A. – REGUERA, P. – FUERTES, J. J. – ALONSO, S. – MORÁN, M.: Cybersecurity training in control systems using real equipment. *IFAC PapersOnLine*, 50 1 (2017), 12179–12184. DOI: https://doi.org/10.1016/j.ifacol.2017.08.2151

[20] BÁNYÁSZ P.: A közösségi média, mint az információs hadszíntér speciális tartománya [Social media as the special part of the information field of operations]. *Hadmérnök*, 12 2 (2017), 108–121.

[21] TÓTH, A.: Future Information Security Threats to the Defense Sector. *Hadtudományi Szemle*, 10 4 (2017), 246–257.

[22] SLIWINSKI, K. F.: Moving beyond the European Union's Weakness as a Cyber-Security Agent. *Contemporary Security Policy*, 35 3 (2014), 468–486. DOI: https://doi.org/10.1080/13523260.2014.959261