TAMAS SOMOGYI,
RUDOLF NAGY

DOI:10.33179/BSV.99.SVI.11.CMC.24.3.1

KIBERNETSKE GROŽNJE IN VARNOSTNI IZZIVI NA PODROČJU FINANC NA MADŽARSKEM

CYBER THREATS AND SECURITY CHALLENGES IN THE HUNGARIAN FINANCIAL SECTOR

Povzetek V zadnjih letih je v bančništvu opaziti naraščanje števila kibernetskih napadov, kar kaže na pomen informacijske varnosti na tem področju. Cilj te študije primera je bolje razumeti informacijsko varnost v okviru zaščite kritične infrastrukture skozi razpravo o izzivih in praksah finančnega področja na Madžarskem. Najprej so v članku opredeljene glavne storitve področja, nato so na podlagi podatkov iz ustrezne literature in poročil organov javne uprave opisane najnovejše kibernetske grožnje za posamezna področja. V zadnjem delu je predstavljen precej izčrpen pregled najpomembnejših točk informacijske varnosti in najboljših praks na podlagi predpisov, priporočil in standardov.

Ključne besede ***Informacijska varnost, kibernetska grožnja, kibernetska varnost, kibernetska odpornost, finančno področje, banka, Madžarska.***

Abstract In recent years an increasing trend has been observed with regard to the number of cyber-attacks in the banking industry, which demonstrates the importance of information security in this sector. The goal of the present case study is to gain a better understanding of information security within critical infrastructure protection by discussing the challenges and practices of the Hungarian financial sector. First, the sector's essential services are identified. Then, the most current sector-specific cyber threats are described, based on data collected from the relevant literature and public authority reports. The final part presents a reasonably comprehensive overview of the key points of information security and best practices based on regulations, recommendations and standards.

Key words ***Information security, cyber threat, cyber security, cyber resilience, financial sector, bank, Hungary.***

Introduction

The daily life of our civilization in this ever-changing world is being threatened more and more as new challenges arise. Besides the traditional security challenges (e.g. the possibility of a wide and devastating war), new challenges have emerged: natural hazards caused by environmental changes, running out of raw materials, the pandemic, to name just a few. Each of these global challenges threatens the infrastructure that serves our accustomed life. Beyond doubt, answering these challenges is crucial from our future's point of view. As politicians and respective experts have realized this, much effort has been made and still is being made in order to identify and protect all the assets needed for essential services.

Besides being a terrible cause of loss of life, the impact of a disruption in essential services or serious damage to the necessary infrastructure is unpredictable. These types of destructive event have diverse effects on the macroeconomy, negatively impacting economic sectors, and thus economic growth, as the findings of Panwar and Sen confirm (Panwar and Sen, 2019). The economic impact is immeasurable, although various disaster impact assessments have been introduced by economic theory (Galbusera and Giannopoulos, 2018). Beyond doubt, these negative economic impacts may provoke economic and social instability, which may cause political instability as well. With regard to the possible political effects of a disastrous event, the consequences of the 9/11 attacks can be mentioned: US homeland security was reorganized and a serious war started (Bullock, Haddow and Coppola, 2020a). Another generally accepted example of possible economic, social and political impacts is the coronavirus pandemic (Karabag, 2020).

To mitigate the severity of these impacts, effective disaster management and resilience is required. The importance of this can be underpinned by the example of the Italian earthquake which struck the Reggio Emilia and Bologna provinces in 2021. A well-coordinated civil protection system, a rapid reorganization of the territory, and strong social networks led to the shortest reconstruction period in Italian history, and to an economic restart despite the ongoing financial crisis (Ghinoi et al., 2021).

As new technologies emerge, governments, law enforcement bodies and disaster management bodies face new challenges. As Cavelty and Wenger (2019) have indicated, political and military actors are attempting to better understand the strategic utility of cyber operations and how to manage intelligence services. Li and Liu (2021) argue that cyberspace and related technologies are one of the most important sources of power. Bullock, Haddow and Coppola (2020b) showed the role of government in cyber security and critical infrastructure protection in the USA, along with the US governmental effort to secure cyberspace.

We live in an increasingly digitalized world; information and communication technology (ICT) has become an inevitable part of our lives, and during the coronavirus pandemic the remote usage of digital services has unexpectedly grown even more. This phenomenon can also be observed in the financial sector: both the

number of financial services offered online and the number of clients using online services are constantly increasing.

Similarly, cybercrime has increased in the past few years (Kerti and Záhonyi, 2020), especially during the coronavirus pandemic as reported by Europol (Europol, 2020). Complex cybercriminal networks operate across the world. Evidence appears to confirm that the use of the *dark web* (a hidden part of cyberspace that provides anonymity for members) is increasing, thus providing more opportunity for malicious activities in cyberspace (Besenyő and Gulyás, 2021). As cyberspace knows no border, nor do the criminals acting worldwide. Beke and Rajnai (2019) remind us that cyber threats have become a worldwide problem, as cyber-attacks can affect users from all over the world. Individuals, businesses, governments and critical infrastructures (CI) are all threatened by cybercrime (Plėta et al., 2020). This is confirmed by Interpol's comprehensive overview of cybercrime during the coronavirus pandemic, which demonstrates that in Europe:

– Widespread phishing campaigns to steal data (including sensitive data) have been registered;
– Official government websites have been cloned and malicious domains have been registered aiming to take advantage of the growing interest in information about Covid-19;
– Ransomware attacks have targeted critical infrastructure and healthcare institutions (Interpol, 2020).

After demonstrating how dangerous a cyber-attack can be, Prevezianou (2020) suggested the introduction of the term »cyber crisis«, and urged the academic world to research this new crisis concept. A study carried out by Koraus et al. (2017) revealed that the majority of people had already encountered cyber-attacks or banking fraud, as ways of shopping had been changed by the expansion of payment cards.

What is remarkable about this overview is that it stresses the fact that cybercrime is a real threat for everyone, especially nowadays, as the usage of online financial services is greater than ever. The impact of a successful cyber-attack against essential services is unpredictable (Tvaronavičienė et al., 2020), so there is an urgent need to better address information security in the financial sector. This case study seeks to describe the cyber threats and information security approaches of the Hungarian banking industry in a comprehensive way (including cyber security and cyber resilience), thus attempting to advance the knowledge of the law enforcement bodies and operators of essential services.

1 FINANCIAL INFRASTRUCTURE

Financial services not only play an essential role in the growth of the economy and well-being of people, but they are also vital for nation-states, as Nagy and Somogyi (2021) revealed. Financial institutions offer a wide array of services and products

to both individuals and large corporations. It is beyond dispute that any significant disruption to these services would have economic, social and political effects which could cross borders and impinge on other EU Member States as well. As Reznik et al. (2020) pointed out, the financial security of the state is fundamental, so significant attention must be paid to it at both the national and international levels.

As Ruvin et al. (2020) claimed, the role of the state in ensuring cyber security in the financial sector by the regulatory framework is fundamental, so national and international regulations concerning cyber threats and information security must be examined when addressing this issue.

In line with EU Council Directive 2008/114/EC, the financial sector in Hungary was identified as a sector providing essential services. Three parts of the financial sector were defined as critical infrastructure (CI) (Act CLXVI of 2012):

– Commerce, payment and clearing of monetary assets and liabilities;
– Security of banks and credit institutions;
– Cash management.

Critical infrastructure protection in the financial sector is regulated by Government Decree 330/2015. The National Bank of Hungary was nominated to take the role of supervisor and control coordinator of critical infrastructure protection in the financial sector. As supervisor, it may call the operator of essential services (OES) to fulfil the relevant requirements; call for the modification of the operational security plan (OSP); or impose a fine. The protection of the identified financial CI should be organized in accordance with the OSP. OESs must appoint a contact person, called a *security liaison officer*, as a single point of contact between the OES and the relevant authorities.

– In addition, emergency cases in the financial sector were defined by Government Decree 330/2015 as:
– The disruption of a control system which has no alternatives within 30 minutes, or where the recovery of the OES must be supported;
– The disruption of ICT or other facility necessary for the fundamental activities which has no alternatives within 1 hour, or where the recovery of the OES must be supported;
– An outage more than one hour long, or a breach of the service level agreement of account management services, e-channel services and cash management;
– An outage more than one day long, or a breach of the service level agreement of cash management;
– Quarantine at the OES;
– An outage of human resources causing a shutdown of CI.

Hence the National Bank of Hungary, as the sector-specific authority, recommends that business continuity plans be created and OES be prepared for the unavailability of the site of operation or of ICT infrastructure (National Bank of Hungary, 2020a).

Taking into consideration these regulations, together with the general expectations of the clients, it can be asserted that financial infrastructure as critical infrastructure must meet the highest recommendations of information security. Moreover, Besenyő and Fehér, in their study of 2020, argue that critical infrastructures become targets of terrorism, including cyber-attacks, so critical infrastructure protection, including information security, must be addressed appropriately.

2 CYBER THREATS IN THE FINANCIAL SECTOR

Hydra, a recently identified malware, targeted those using the online banking services of the German Commerzbank. As the National Cyber Security Centre of Hungary described the case in its weekly newsletter, a fake homepage was used to share the camouflaged malware (National Cyber Security Centre, 2021). This case is not extraordinary. The European Central Bank (ECB), as a sector-specific supervisor in Europe, has observed[1] an increasing trend in the number of cyber incidents in the last few years. As the ECB pointed out: »*40% of the banks were the target of at least one successful cyberattack in 2019, a considerable increase from the 28% reported in 2018*« (European Central Bank, 2021, 5th paragraph).

The general picture emerging from the analysis of the cyber incidents is that the vast majority of cases involved malicious and criminal intent. Analysis of the reported cyber incidents in 2019 shows that phishing attacks against financial institutions or customers were the most frequent type of incident, followed by denial-of-service attacks (generally Distributed Denial of Service – DDoS – which involves a large number of raiders at the same time). The purpose of DDoS attacks is to cause an interruption to services by flooding the servers with mass requests. A variant of the DDoS attack has also been observed, where the perpetrators threatened financial institutions with a DDoS attack unless a ransom was paid (European Central Bank, 2021). DDoS attacks became the most frequent cyber incidents in 2020 (European Central Bank, 2020).

Naturally, other types of attacks also have to be taken into consideration, including the 'man-in-the middle' (criminals insert themselves between the customer and the bank to steal information or manipulate transactions), and the 'zero-day exploit' (criminals taking advantage of a vulnerability in a used software before the vendor is able to fix it) (BIS, 2021).

[1] *Significant cyber incidents are reported to the ECB through the cyber incident reporting framework as soon as they are detected, so trends can be identified and monitored by the supervisor.*

Besides the emergence of cyber risks, another trend can also be observed: reliance on outsourced ICT services is steadily growing. Today banks increasingly use third-party providers (e.g. cloud service providers and consultants) in order to provide more and a higher level of services. Cooperation between financial institutions and FinTech (financial technology) companies is gradually growing. Undoubtedly, providing better services and using new technologies is advantageous for both the financial institutions and their clients. However, the overall ICT risk has sharply increased:

– Third parties have discovered incidents roughly as often as banks (European Central Bank, 2020), meaning that these third-party providers are also facing cyber-attacks, just like financial institutions do;
– Supply chain risk (criminals attempting to insert malware into ICT systems by the access supply chain) must also be taken into consideration, as the consequence of this risk may be damage to the integrity of ICT services (National Counterintelligence and Security Centre, 2020).

A particular manifestation of the challenges to the banking system was observed in the 2008 Russia-Georgia war, during the course of which, guided by the intention to cause social disturbance to facilitate armed military operations, a coordinated hacker attack hit the Georgian banking system (Besenyő, 2008). Similarly, in their study Zachosova and Babina (2018) found that the financial sector of Ukraine has also faced non-traditional threats since the conflict in East Ukraine.

It is worth adding that these potential and already implemented attacks may have different purposes (fraud, espionage, activism/sabotage, cyber terrorism), and may use a variety of techniques (e.g. social engineering, intrusion attempts through the exploitation of vulnerabilities, deployment of malicious software).

Seeking to address the cyber threats of the financial sector, the European Banking Authority (EBA) has issued *Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process* (European Banking Authority, 2017). In order to promote a common methodology for assessing ICT risks, the EBA Guidelines support the notion of grouping ICT cyber risks as:

– Cyber-attacks and other external ICT-based attacks (attacks through the internet or outside networks resulting in control being taken of internal ICT systems; execution of fraudulent transactions by hackers; attacks on communication connections and conversations);
– Inadequate internal ICT security (gaining unauthorized access to critical ICT systems; unauthorized manipulations; security threats due to a lack of security awareness; the unauthorized storage or transfer of confidential information);
– Inadequate physical ICT security (misuse or theft of ICT assets; deliberate or accidental damage to physical ICT assets; insufficient physical protection against natural disasters);

– Disruptive and destructive cyber-attacks (attacks which result in the overloading of communication and information systems and the network, preventing services from being accessed).

Taken altogether, the data and trends presented above provide evidence that cyber threats are an increasing challenge for the financial sector. In a digitalized world such as that we live in today, cyber incidents are inevitable. However, the financial sector, as critical infrastructure, must take action to mitigate the associated risks. This responsibility is considerable; in many cases, these cyber incidents received both local and national media coverage, potentially affecting the banks' reputation and eventually also trust in the national CI as a whole. Some incidents were even reported in the international press (European Central Bank, 2020), bringing an international focus to the issue.

After this description of the current cyber threats, it is necessary to examine the key points of the information security applied in the Hungarian financial sector.

3 INFORMATION SECURITY IN THE FINANCIAL SECTOR

In addressing the issue of information security, Hungarian financial institutions follow the recommendations of the National Bank of Hungary. As a sector-specific authority, the National Bank summarizes the basis of ICT protection in its Recommendation No. 8/2020 (National Bank of Hungary, 2020a). Besides this recommendation, the best practices of the financial sector are based on relevant case studies, audit findings, the results of various types of test, and industry standards (e.g. the ISO/IEC 27000 series on information security questions; ISO/IEC 22237 on data centre facilities and infrastructures).

A comprehensive list of answers to information security challenges clearly consists of the following solutions in order to reduce the risk of a successful attack and be ready to respond at all times. It must be noted that a holistic approach is required in order to build up effective information security; cyber defence, cyber security and cyber resilience must be taken into consideration together.

3.1 Training and education

Callies and Baumgarten (2020, p 1154) highlighted the significance of the human element in security: »*Often, businesses and institutions are overly focused on technological security and software, but they neglect company culture, people, and processes. The human element, however, is still the weakest link when it comes to cybersecurity*«. This has been recognized by the legislators; provisions for regular mandatory security training in the financial sector have been included in Government Decree 42/2015. The National Bank of Hungary recommends that security training be held on an annual basis (National Bank of Hungary, 2019).

Phishing attacks, one of the most frequent types of cyber-attacks (as mentioned above), try to deceive people. Improving resistance to phishing attacks involves education; staff must be familiar with the importance of recognition and the fast escalation of a phishing attack. Although email-based phishing is currently the principally used deceptive attack, other types must also be mentioned. People working in the financial sector must also be prepared for *vishing* (voice phishing over the phone) and *smishing* (SMS phishing), and certain officers and managers must be well prepared for *spearphishing* (targeting specific people), *whaling* attacks (targeting senior managers or board members) and *honey traps* (attackers pretending a romantic interest).

Kárász and Négyesi (2020) established a link between the security awareness of an operator of essential services and the engagement of the management; employee awareness is based on the awareness level of the management. Therefore, the more engagement by the top management in critical infrastructures, the higher level of information security awareness. In order to provide an experimental and practical learning opportunity through game play, Legárd (2021) outlined several gaming models for training, and drew up a plan for an information security awareness raising application.

It must be noted that, according to the aforementioned Government Decree 42/2015, training is mandatory for everyone involved in the operation or use of ICT systems in production. Moreover, in order to ensure the appropriate high level of knowledge of security experts in financial institutions, special training must be organized for those working in the field of cyber security. As a best practice, financial institutions require that certain staff members have a relevant certificate, or support the staff in acquiring a certificate. It is worth mentioning that sector specific training is provided in Hungary by the national association of the staff of financial institutions.

3.2 Simplifying the ICT landscape – segmenting the network

Financial institutions and Fintech companies are continually developing digital technologies and competing to roll out new services. However, increasing the attack surface has been identified as a cyber risk. Financial institutions must aim to reduce the possible entry points of unauthorized access into the ICT infrastructure.

Furthermore, the network must be segmented, and each segment must have only the minimum number of necessary gates. In the event of an unauthorized access to a certain network segment, all the other segments can be protected by cutting off the minimal access points between them.

In order to be effective, security must be built in to both the hardware and software levels. The *security by design* principle must be taken into consideration to have the right level of security from the very beginning, in order to treat the root cause and not the symptom. However, security decision-making is difficult for new system designs, since there is no past experience that can be taken into consideration. Meland et al.

described a threat likelihood estimation approach to support decision-making for new system designs (Meland et al., 2022).

Additionally, it must be noted that the increasing number of services provided by the financial sector necessarily involves the use of some cloud-based services. Besides the cloud-specific recommendations of the National Bank of Hungary (National Bank of Hungary, 2019), the sector-specific authority also recommends that the cloud service provider's controls for data protection and cyber security be supervised by the financial institution (National Bank of Hungary, 2020a).

3.3 Appropriate, tested procedures

Procedures must exist and be applied and continuously improved in order to prevent

- Unauthorized access to ICT systems;
- Unauthorized use of ICT infrastructure;
- Unauthorized manipulation of data or the system configuration;
- Unauthorized storage or transfer of confidential information.

A notable example of procedure with regard to authorized access to ICT systems is password management, which is an important part of information security. A study by Kadena (2019) administered a survey to university students enrolled in ICT studies to determine the habit of password selection. Kadena's findings provide convincing evidence that even ICT people tend to neglect the use of strong passwords. In financial institutions, password management must force the use of strong passwords. Regular password cracking exercises run by the security operators of the financial institution can ensure that weak passwords are not used in the organization.

Besides these procedures, financial institutions must also have thorough procedures for identifying risks and for taking the appropriate action in order to avoid having a risk without a proper countermeasure. Besides the aforementioned EBA Guidelines on ICT risk assessment (European Banking Authority, 2017), the international standard of ISO 31000 on risk management can also be used.

It must be mentioned that these procedures must be regularly audited and, if required, modified in accordance with the audit findings. Moreover, incidents, losses, changes in the industry standards, and the results of test exercises must all be analyzed and used as input for improving the procedures.

The National Bank of Hungary recommends that the aforementioned procedures exist and that staff are trained in them in a documented manner (National Bank of Hungary, 2020a). Undoubtedly, ICT and information security governance must include all the procedures, principles and standards concerned with setting the financial institution's objectives, strategies and risk management framework.

3.4 Tools of security, defence and resilience

Undoubtedly, state of the art technology must be applied in the field of information security. The most modern tools that have been installed in the financial institutions can be categorized as:

- *Endpoint protection* to detect and block suspicious activity at endpoints (e.g. antivirus and data leakage protection);
- *Endpoint detection and response* to monitor and detect suspicious activity at endpoints (e.g. virus scanning and labelling as part of the data leakage protection system);
- *An intrusion detection system* to monitor and detect suspicious activity in the network or in an ICT system (e.g. host intrusion detection system);
- *An intrusion prevention system* to respond to suspicious activity in the network or in an ICT system (e.g. firewalls);
- *A honeypot* as a decoy to attract cyber criminals who then spend time and effort on nothing really important while their activity is monitored and analyzed;
- *DDoS protection* to protect online services against disruptive and destructive cyber attacks;
- *An incident management system* to support the management tasks of a security incident;
- *A backup system* to store data in a safe way in order to be able to recover data if required.

These tools aim to support the high level of security, defence (by preventing the disruption or destruction of the services and by inhibiting cyber criminals from gaining control over the ICT systems), and resilience (by being able to respond to and recover from a cyber incident and resume business operations). Moreover, by using honeypots, information on the cyber criminals and their techniques can be gained to improve the level of security and the capability of a fast and successful recovery. A honeypot-based approach for intrusion detection/prevention systems has been proposed by Baykara and Das (2018), in order to analyze information in real time.

As described above, backup systems provide the ability to restore data, which is an important aspect of cyber resilience. It must be noted that special backup solutions are applied to data considered the most important, based on an appropriate assessment: *immutable backup solutions.* These data storage solutions refer to technology against malicious attacks aiming to destroy data by deletion, modification or encryption.

Confidential, sensitive and personal data are stored, processed and transferred in the financial sector, so communication channels must also be protected. Applying appropriate actions to ensure the confidentiality and integrity of data transferred through communication channels is expected by the National Bank of Hungary (2020a).

It is worth adding that an appropriate level of security solutions must also be applied in the case of home offices (National Bank of Hungary, 2020b). The importance of the issue of home offices has increased since the beginning of the Covid-19 pandemic, so future studies will have to continue to explore the questions of *home offices* and *bring your own device* possibilities in the financial sector to deal with the risk of data leakage. The importance of this issue has been observed by Michelberger (2020), who suggested an appropriate security framework.

3.5 Partnership and information sharing

Undoubtedly, extensive partnership has already been established. Information sharing takes place within the national association of financial institutions, where the sector-specific authority is also represented. This body also serves as a link between the sector and the legislators.

Financial institutions cooperate with external auditors and companies from the field of security. The level of cyber security and cyber resilience can be increased through companies with broad international experience, for example, through the findings of independent auditors. Ethical hackers also may contribute to raising cyber security and cyber resilience to the highest levels. The *red team exercise* refers to a case where ethical hackers test the financial institution's defence by attacking the company. The time of the attack and the method is unknown to the security experts of the financial institution (who are referred to as the *blue team*). *Purple team exercises* refer to a case when internal (blue team) and external (red team) experts join together for a period of time to analyze part of the financial institution's security lines and solutions. These exercises are also an opportunity to try out and improve crisis and incident management.

It is important to note that sharing information about the big picture of information security is dangerous. It is therefore highly advisable to cooperate with various partners within this field, and to share information about and provide access for each partner only to different parts of the entire information security system. The same caution is suggested in the case of staff members; knowing the big picture is not necessary for them.

As already mentioned, all the Hungarian OESs appoint a security liaison officer to act as a single point of contact between the OES and the relevant disaster management bodies. Clear roles in government institutions and the financial sector members lay the ground for appropriate communication during preparation, test exercises, and in the event of a real security incident. Recognizing the importance of this role, the qualifications of the security liaison officer are specified by Act CLXVI of 2012.

3.6 Physical security

Few attempts have been made to explore the role of physical security within the field of information security. However, ICT systems undoubtedly represent a considerable

part of the financial institutions' assets, which must be protected, so physical security must also be addressed. Physical access to the ICT infrastructure creates a twofold risk: the first is the risk of the destruction or theft of the ICT infrastructure elements, and the second is the risk of attacks on communication connections and conversations, or the taking control of ICT systems.

These risks must also be taken into account to improve the level of information security. A high level of physical security has been recommended by the National Bank of Hungary (2020a). In addition to this recommendation, relevant parts of the standard ISO/IEC 22237 on data centre facilities, just like the standard of ISO/IEC 30104 on hardware security assurance, are also to be applied within the field of physical security.

Conclusion

Technological innovation plays a crucial role in the financial sector from a strategic standpoint and as a source of competitive advantage. New digital services are continually being offered by financial institutions to an increasing number of customers. Nevertheless, cyber crime has also been increasing in the world, as pointed out by respective international law enforcement bodies and relevant studies. Taking into account the potential impact of a significant disruption to the essential services of the financial sector, there is no doubt that critical infrastructure protection and information security must be addressed appropriately.

To gain a better understanding of the security challenges, the current sector-specific cyber threats were explored. Analyzing the public reports of the relevant authorities, this study found that phishing and DoS are the most common cyber-attacks, while the risk of inadequate ICT and physical security and the supply chain risk must also be taken into consideration.

Seeking answers to these challenges, the key elements of information security were explored. Examining the best practices, regulations and standards, this study has identified the following key elements of information security applied in the financial sector in Hungary: training and education; a simple ICT landscape; appropriate procedures; state-of-the art tools arranged in a comprehensive and multi-layered way; suitable partnership between sector members; and physical security.

This study was undertaken to provide an overview of the cyber threats and best practice security solutions applied in the Hungarian financial sector in order to contribute to the development of information security within critical infrastructure protection.

Bibliography

1. *Baykara, M., and Das, R., 2018. A novel honeypot based security approach for real-time intrusion detection and prevention systems. Journal of Information Security and Applications. Vol 41, pp 103–116. 2018. ISSN 2214-2126.*
2. *Beke, É., and Rajnai, Z., 2019. Global and European cyber defence framework and recommendations. In: Rajnai Z. (Ed.) Kiberbiztonság/Cybersecurity. Biztonságtudományi Doktori Iskola, Budapest, pp 123–136. ISBN 978-963-449-185-9.*
3. *Besenyő, J., 2008. A new kind of war? Internet warfare in Georgia. Army Review, Vol 6, No 3, pp 61–63., 2008.*
4. *Besenyő, J., and Fehér, A., 2020. Critical infrastructure protection (CIP) as new soft targets: private security vs. common security. Journal of Security and Sustainability Issues. Vol 10, No 1., pp 5–18. 2020. ISSN 2029-7025.*
5. *Besenyő, J., and Gulyas, A., 2021. The effect of the dark web on security. Journal of Security and Sustainability Issues. 2021, Vol 11, pp 103–121. ISSN 2029-7025.*
6. *BIS bulletin No. 37., 2021. Covid-19 and the cyber risk in the financial sector. Bank for International Settlements Bulletin. 14 January, 2021. ISBN 978-92-9197-451-0, https://www.bis.org/publ/bisbull37.pdf, 24 Nov 2021.*
7. *Bullock, J. A., Haddow, G. D., and Coppola, D. P., 2020a. Chapter 1 – Homeland security: the concept, the organization. In: Introduction to Homeland Security, pp 1–34. 2020. ISBN 978-0-12-817137-0.*
8. *Bullock, J. A., Haddow, G. D., and Coppola, D. P., 2020b. Chapter 8 – Cyber security and critical infrastructure protection. In: Introduction to Homeland Security, pp 425–497. 2020. ISBN 978-0-12-817137-0.*
9. *Calliess, C., and Baumgarten, A, 2020. Cybersecurity in the EU – the Example of the Financial Sector: A Legal Perspective. German Law Journal, Vol 21, No 6, pp 1149–1179.*
10. *Cavelty, M. D., and Wenger, A., 2019. Cyber security meets security politics: complex technology, fragmented politics and networked science. Contemporary Security Policy. Vol 41, No 1, pp 5–32. 2020. ISSN 1743-8764.*
11. *European Banking Authority, 2017. Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP). 11 May 2017, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-48a1-8208-3b8c85b2f69a/Final%20Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29.pdf?retry=1, 24 Nov 2021.*
12. *European Central Bank, 2020. Guarding Against IT and Cyber Risk. 13 May 2020, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2020/html/ssm.nl200513_1.en.html, 24 Nov 2021.*
13. *European Central Bank, 2021. Supervision Newsletter, IT And Cyber Risk: A Constant Challenge. 18 August 2021, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2021/html/ssm.nl210818_3.en.html, 24 Nov 2021.*
14. *Europol, 2020. Covid-19 sparks upward trend in cybercrime. Press release 5 October 2020, https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime, 24 Nov 2021.*
15. *Galbusera, L., and Giannopoulos, G., 2018. On input-output economic models in disaster impact assessment. International Journal of Disaster Risk Reduction. Vol 30, pp 186–198. 2018. ISSN 2212-4209.*
16. *Ghinoi, A., Righi, E., Lauriola, P., Giovanetti, E., and Soldati, M., 2021. Disaster risk reduction and interdisciplinary education and training. Progress in Disaster Science. Vol 10. 2021. ISSN 2590-0617.*
17. *Interpol, 2020. Cybercrime: Covid-19 impact. August 2020, https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf, 24 Nov 2021.*

18. *Kadena, E., 2019. Password selecting habits. In: Rajnai, Z. et al. Kiberbiztonság - Cybersecurity 2. Biztonságtudományi Doktori Iskola. Budapest. 2019, pp 161–175. ISBN 978-963-449-185-9.*
19. *Karabag, S. F., 2020. An unprecedented global crisis, the global, regional, national, political, economic and commercial impact of the coronavirus pandemic. Journal of Applied Economics and Business Research. Vol 10, No 1, pp 1–6. ISSN 1927-033X.*
20. *Kárász, B., and Négyesi, I., 2020. Information security responsibilities of critical (information) infrastructures in the aspect of human risk factors. Hadtudományi Szemle. Vol 13, No 3, pp 71–86. 2020. ISSN 2060-0437.*
21. *Kerti, A., and Záhonyi, L., 2020. A study of the history of information security – incidents, methods, standards and trends. National Security Review. Issue 2/2020, pp 176–189. ISSN 2063-2908.*
22. *Koraus, A., et al., 2017. The safety risks related to bank cards and cyber attacks. Journal of Security and Sustainability Issues. Vol 6, No 4, pp 563–574. ISSN 2029-7025.*
23. *Legárd, I., 2021. A game for the future: possibility of developing information security awareness with the help of a gamified application. Polgári szemle. Vol 17, No 1-3, pp 358–373. 2021. ISSN 1786-6553.*
24. *Li, Y., and Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security: emerging trends and recent developments. Energy Reports. Vol 7, pp 8176–8185. 2021. ISSN 2352-4847.*
25. *Meland, P. H. et al., 2022. Assessing cyber threats for storyless systems. Journal of Information Security and Applications. Issue 64, 2022. ISSN 2214-2126.*
26. *Michelberger, P., and Fehér-Polgár, P., 2020. BYOD security strategy (aspects of a managerial decision). Journal of Security and Sustainability Issues. Vol 9, No 4, pp 1135–1143. 2020. ISSN 2029-7025.*
27. *Nagy, R., and Somogyi, T., 2021. The financial infrastructure as a critical infrastructure and its specialities. National Security Review. Issue 2/2021, pp 213–223. ISSN 2063-2908.*
28. *National Bank of Hungary, 2019. Recommendation No 4/2019 (IV.1.), https://www.mnb.hu/letoltes/4-2019-felho.pdf, 24 Nov 2021.*
29. *National Bank of Hungary, 2020a. Recommendation No 8/2020 (VI.22.), https://www.mnb.hu/letoltes/8-2020-informatikai-rendsz-vedelmerol.pdf, 24 Nov 2021.*
30. *National Bank of Hungary, 2020b. Recommendation No 12/2020 (XI.6.), https://www.mnb.hu/letoltes/12-2020-tavmunka-ajanlas.pdf, 24 Nov 2021.*
31. *National Counterintelligence and Security Centre, 2020. Supply Chain Risk Management. 25 September, 2020. Office of the Director of National Intelligence, https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf, 24 Nov 2021.*
32. *National Cyber Security Centre, 2021. Weekly Newsletter. 41/2021, https://nki.gov.hu/wp-content/uploads/2021/10/Sajtoszemle_41.het_.pdf, 24 Nov 2021.*
33. *Panwar, V., and Sen, S., 2019. Economic impact of natural disasters: an empirical re-examination. Margin: The Journal of Applied Economic Research. Vol 13, No 1, pp 109-139. 2019. ISSN 0973-8029.*
34. *Plėta, T., Tvaronavičienė, M., Della Casa, S., and Agafonov, K. 2020. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development, 2(3), pp 703–715. https://doi.org/10.9770/IRD.2020.2.3(7).*
35. *Prevezianou, M. F., 2020. Beyond ones and zeros: conceptualizing cyber crises. Risk, Hazards & Crisis In Public Policy. Vol 12, No 1, pp 51–72. ISSN 1944-4079.*
36. *Reznik, O., et al., 2020. Financial security of the state. Journal of Security and Sustainability Issues. 2020. Vol 9, No 3, pp 843–852. ISSN 2029-7025.*

37. *Ruvin, O., et al., 2020. Cybersecurity as an element of financial security in the conditions of globalization. Journal of Security and Sustainability Issues. Vol 10, No 1, pp 175–188. 2020. ISSN 2029-7025.*
38. *Tierney, K., 2012. Disaster governance: social, political and economic dimensions. Annual Review of Environment and Resources. Vol 37, pp 341–363. 2012. ISSN 1543-5938.*
39. *Tvaronavičienė, M., Plėta, T., Della Casa, S., and Latvys, J. 2020. Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of the USA, the UK, France, Estonia and Lithuania. Insights into Regional Development, 2(4), pp 802–813. http://doi.org/10.9770/IRD.2020.2.4(6).*
40. *Zachosova, N., and Babina, N., 2018. Identification of threats to financial institutions' economic security as an element of the state financial security regulation. Baltic Journal of Economic Studies. 2018. Vol 4, No 3, pp 80–87. ISSN 2256-0963.*

e-mail: somogyi.tamas@phd.uni-obuda.hu
e-mail: nagy.rudolf@uni-obuda.hu

e-mail: somogyi.tamas@phd.uni-obuda.hu

Mag. Tamas Somogyi je magistriral iz informacijskega inženiringa in dodatno še iz pravnih študij. Ima več kot deset let izkušenj na področju informacijske tehnologije v bančništvu in je zaposlen v drugi največji banki na Madžarskem kot vodja operativnega tveganja, odgovoren za obnovitev po nesreči. Poleg tega je trenutno doktorski študent na doktorski šoli za varnostne vede na univerzi Óbuda.

Tamas Somogyi, MSc, holds a Master's degree in IT engineering and a complementary degree in Legal Studies. Having more than ten years of experience in the field of IT within the banking industry, he is working for the second largest bank in Hungary as an operational risk manager, being responsible for disaster recovery. Besides this, he is currently a PhD student at the Doctoral School on Safety and Security Sciences, Óbuda University.

e-mail: nagy.rudolf@uni-obuda.hu

Dr. Rudolf Nagy, polkovnik v pokoju, je trenutno docent na univerzi v Óbudi. Bil je častnik za JRKB-obrambo in sodeloval pri nalogah zagotavljanja varstva pri delu. Izkušnje je pridobival kot operativni častnik v Natovi misiji Sforja. Pozneje je bil namestnik vodje oddelka za obvladovanje izrednih razmer pri madžarskem nacionalnem generalnem direktoratu za obvladovanje nesreč. Od leta 2015 poučuje predmete s področja varstvoslovja in je odgovoren za specializacijo iz protipožarnega inženiringa.

Dr Rudolf Nagy, ret. Col., is currently Assistant Professor at Óbuda University. He was a CBRN defence officer, and took part in industrial safety tasks. He gained experience as an operations officer in the NATO SFOR mission. After that he became Deputy Head of the Emergency Management Department of Hungarian National Directorate General for Disaster Management. He has been teaching subjects of safety and security sciences since 2015, and is responsible for the fire protection engineering specialization.