Tamás Somogyi,
Rudolf Nagy

DOI: 10.2478/cmc-2023-0020

VPLIV VOJNE V UKRAJINI NA INFORMACIJSKO VARNOST BANČNEGA SEKTORJA EVROPSKE UNIJE – ŠTUDIJA PRIMERA MADŽARSKE IN SLOVAŠKE

THE IMPACT OF THE WAR IN UKRAINE ON THE INFORMATION SECURITY OF THE EUROPEAN UNION'S BANKING INDUSTRY – A CASE STUDY OF HUNGARY AND SLOVAKIA

Povzetek V študiji prvič preučujemo vpliv vojne na informacijsko varnost bančnega sektorja EU. To področje je ključnega pomena, saj lahko hujši kibernetski incident povzroči finančno in politično nestabilnost držav članic in je učinkovitost finančnih sankcij, ki jih je sprejela EU, odvisna od ustreznega delovanja bančnih sistemov EU. Uporabljene so kvalitativne metode: analiza ustrezne literature in javno dostopnih podatkov za posamezne sektorje, opravljeni razgovori z višjimi strokovnjaki za informacijsko varnost iz madžarskih in slovaških bank. Rezultati potrjujejo, da se banke v EU soočajo z izjemno visoko ravnjo kibernetskega tveganja. Članek navaja ukrepe za odzivanje na omenjena tveganja z namenom ohranjanja varnosti.

Ključne besede ***Ukrajina, Rusija, informacijska varnost, Evropska unija, bančništvo.***

Abstract This study investigates, for the first time, the impact of the war on the information security of the EU's banking industry. This domain is critical, as i) a significant cyber incident may lead to the financial and political instability of the Member States, and ii) the efficiency of the financial sanctions adopted by the EU depends on the appropriate operation of the EU's banking systems. Qualitative methods were used in the study; relevant literature and publicly available sector specific data were analysed, and senior information security experts from Hungarian and Slovakian banks were interviewed. The results underpin the fact that banks in the EU are facing an exceptionally high level of cyber risk; the paper attempts to provide actions responding to these risks to keep the banking industry secure.

Key words ***Ukraine, Russia, information security, European Union, banking industry.***

Introduction

Besides the constant threat of cyber terrorism (Kenney, 2015), guided cyber-attacks have been experienced in recent conflicts, e.g. in Georgia (Besenyő, 2008) and in Estonia (Blank, 2008). An analysis of Russia's war in Georgia foresaw the possible further diversification of Russian military capabilities, among which is an increase in the ability to carry out information warfare operations (Pallin and Westerlund, 2009). Furthermore, the stealing of US national security secrets (probably by China and Russia) has been suggested (Blair and Roth, 2022). Other examples, such as the distributed denial of service (DDoS) attacks on the US financial sector in 2012 (probably supported by Iran), and the decades-long economic espionage against US corporations (probably by China), underpin the fact that NATO has identified cyberspace as a domain of operations (Reveron and Savage, 2020).

As is generally accepted, individuals, businesses, governments and critical infrastructures are all threatened by cyber-attacks (Pléta et al., 2020). The significance of critical infrastructure can be understood by its definition given by European Council Directive 2008/114/EC Article 2: "…*essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people…*". The possible surface that can be attacked is constantly growing as technology spreads (Costigan, 2016). Undoubtedly, the impact of a successful cyber-attack against the essential services provided by critical infrastructure is unpredictable. It has been demonstrated that this domain has already been considered a possible target by cyber terrorists (Besenyő et al., 2021; Besenyő and Kovács, 2023).

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. Taking into consideration the networks of parent and subsidiary companies in the banking industry, this kind of effect can easily cross borders and impinge on other States as well. Financial services not only play an essential role in the growth of the economy and well-being of people, but also vital to States, so the services of the banking industry should be considered essential services (Nagy and Somogyi, 2021). Since banks offer digitalized services and operate through critical infrastructure, the banking industry is increasingly vulnerable, as has been demonstrated by Kohler et al. (2021). Among the potential hybrid threats against an EU Member State, a significant cyber-attack against the finance sector has already been identified (Hugyik, 2020). The information security of the banking industry can therefore be seen as fundamental (Somogyi and Nagy, 2022).

Furthermore, the European banking system – in certain ways – has been involved in the ongoing war. Firstly, in reacting to the Russian invasion the European Union has adopted restrictive measures against Russia and Belarus, which have been implemented by European banks. Secondly, as investors have taken the war seriously, European stock markets began to react negatively (Ahmed et al., 2022), creating an economic environment in which the stable operation of the financial sector is necessary to avoid additional panic among investors. Moreover, as wars have great social impact (Rácz, 2020), social and political stability also depends on the secure

operation of the banking industry. Thus, by playing a critical role in this conflict, the European banking industry and its information security has become one of the central issues of recent defence studies. This paper makes a contribution to this field by offering insights into the most current issues in cyber security in the Hungarian and Slovakian banking industry.

1 METHODS

This study employed a qualitative approach which involved a literature review and research using publicly available data published by sector specific supervisors. In addition to this, semi-structured interviews were conducted with senior information security experts from Hungarian and Slovakian banks in the second half of 2022. Although the issue of information security (especially during an ongoing war) is strictly confidential, some experts were willing to participate in these interviews. Due to the sensitivity of the collected data, the interview results are provided anonymously, without mentioning confidential data or any tangible information security solutions. The purpose of the Hungarian and Slovakian examples provided is to gain insight into the information security challenges faced by the banking industry, so the list of examples is not complete; however, some of them can be generalized for the entire sector.

Hungary and Slovakia were chosen because both countries are members of both the EU and NATO; they are direct neighbours of Ukraine; and they are catering for refugees and supporting the Ukraine in various ways.

2 OVERVIEW OF THE MANAGEMENT OF CYBER RISKS IN THE EUROPEAN BANKING INDUSTRY

In general, cyber-attacks against the banking industry may have different purposes (fraud, espionage, activism, sabotage, 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* (EBA, 2017). In order to promote a common methodology for assessing ICT risks, the EBA Guidelines support the idea of grouping the ICT cyber risks as follows:

1. Cyber-attack and other external ICT-based attacks (attacks carried out via the internet or outside networks resulting in the loss of control of internal ICT systems; fraudulent transactions by hackers; attacks on communication connections and conversations),
2. Inadequate internal ICT security (gaining unauthorized access to critical ICT systems; unauthorized manipulation; security threats due to lack of security awareness; the unauthorized storage or transfer of confidential information),

3. Inadequate physical ICT security (misuse or theft of ICT assets; deliberate or accidental damage to physical ICT assets; insufficient physical protection against natural disasters),
4. Disruptive and destructive cyber-attacks (attacks which result in an overloading of communication and information systems and the network, preventing services from being accessed).

Taking action to appropriately mitigate cyber risks is an increasing challenge of the banking sector. This responsibility is considerable; cyber incidents in the banking industry may receive both local and national media coverage, potentially affecting the banks' reputation and eventually also the trust in the national critical infrastructure as a whole, or affecting trust in democratic institutions and political leaders. Some incidents may even be reported in the international press, and may also have political effects.

Having realized the importance of the information security of the banking industry, the following question should be posed: "Have the cyber threats of the banking industry changed due to the war?" or, in other words, "Does the war have any impact on the security of the IT infrastructure of the financial sector?"

3 CYBER RISKS IN THE EUROPEAN BANKING INDUSTRY DURING THE WAR

Before examining the cyber threats due to the ongoing war in Ukraine, it is necessary to describe the situation just before the war. The European Central Bank, as a sector-specific supervisor in Europe, has observed an increasing trend in the number of cyber incidents in recent years (European Central Bank, 2021). This increase in cyber-crime was particularly noted during the coronavirus pandemic, as reported by Europol (Europol, 2020). These data show that there had been a steady growth in cyber threats to the IT infrastructure of the European banking industry before the outbreak of war in February 2022.

Prior studies have shown that during the conflicts and wars in which Russia has participated over the past decades the banking industry has faced many more cyber-attacks than usual. For instance, during the war in Georgia in 2008 a coordinated hacker attack hit the Georgian banking system (Besenyő, 2008), and since the conflict in the eastern parts of Ukraine the financial sector has faced additional cyber threats (Zachosova and Babina, 2018). These examples underpin the idea that Russia has been conducting non-military operations as well, in line with the so-called "Gerasimov doctrine", in order to achieve its own political and strategic goals (Štrucl, 2022).

Interviews with senior experts from the banking industry in Slovakia and Hungary verify that the already high level of cyber threats against the banking industry has grown even higher since the outbreak of the war in Ukraine. This rise has also been highlighted by a member of the European Central Bank's supervisory board

(Tuominen, 2022). Thus, the banking industry is facing an increased level of cyber risk, as the European Central Bank has also pointed out (European Central Bank, 2022a). Managing these cyber risks is an increased challenge for the banking industry, since it is causing overwork and unexpected costs. Nevertheless, as has been suggested by the European Central Bank, European banks need to remain on high alert to identify cyber risks and to be prepared to address them (European Central Bank, 2022b). These cyber risks will now be examined based on the aforementioned categories defined by the EBA.

The first category of cyber risk is cyber-attacks aiming to take over the control of internal ICT systems. Two main factors have increased the probability of such a cyber-attack: first, the European sanctions against the Russian Federation have closed or limited its access to the international banking system (e.g. SWIFT) and access to Russian bank accounts in European banks, and second is the idea that successfully manipulating payment transactions from the EU to Ukraine would weaken the Ukrainian resistance and undermine its political stability. This underlines the importance of appropriate protection. Besides the already existing security measures, what new actions can be suggested in order to decrease the risk of takeover of control of ICT systems?

– One expert from a Hungarian bank revealed that one of their high priorities is to accurately check whether the financial sanctions are being observed. The importance of such extra or new monitoring actions has also been emphasized by the National Bank of Hungary (National Bank of Hungary, 2022).
– One interviewee indicated that in a Slovakian bank the idea of shutting down software which is supported or was developed by Russian developers has been discussed, as a built-in hidden communication channel or an as-yet unidentified vulnerability could result in a loss of control of ICT systems.

The second category of ICT risk is an inadequate level of internal information security, which could result in unauthorized access to ICT systems and manipulation of data. Taking into consideration European sanctions impacting Russian payment transactions, the risk of bribery and blackmail by Russian intelligent services could be higher, hence the importance of internal information security. Besides the already existing actions, some new measurements may be suggested in order to strengthen information security:

– New anti-fraud actions with regard to staff in relevant positions (e.g. authorized to confirm international transactions);
– Rigorous checks of the sanctions' implementation, especially in Hungary, where a domestic instant payment service is available;
– Additional inner audit of relevant processes and staff;
– Enhanced monitoring capability of information security events.

The third category is the management of physical security and physical ICT security, which is also essential. Inappropriate access to ICT assets may lead to i) physical

damage to critical infrastructure elements, or ii) the manipulation of ICT hardware elements in order to carry out espionage or other malicious activities. Since the war, the risk of a politically motivated attack on banks is higher, so the already existing physical security measures should be enhanced.

– Taking into consideration the close proximity of Hungary and Slovakia, the possibility of bank robbery or attacks against ATMs located near the Ukrainian border is higher. For instance, should a group cross the border illegally (e.g. escaping from military service or from prison impacted by military activities), they would certainly need cash. Therefore, a more cautious operation of branches and ATMs can be advised, e.g. decreasing the amount of money stored in ATMs;
– An attack could be launched by extremists on critical infrastructure in general, including on the infrastructure of the banking sector. As discussed in the Introduction, European banks are implementing the sanctions adopted by the European Union, so they may be considered as an 'enemy' by some extremists. According to a Hungarian interviewee, the issue of physical security with regard to the protection of branches and ATMs has been discussed in Hungary with the relevant members of the defence sector.

The fourth category of IT risk is the risk of disruptive and destructive cyber-attacks resulting in service unavailability. As has been described in the Introduction, the services of the banking industry can be considered essential, especially during a war, hence the importance of preparedness for disruptive cyber-attacks, which can be enhanced by the following actions:

– Extra attention should be paid to DDoS protection, as this type of cyber-attack against the banking industry has already been experienced since the war, in Estonia in June, as reported by the relevant Estonian authority (Information System Authority, 2022);
– Interviewees have confirmed the necessity of security awareness with regard to emails or calls disturbing the daily operation of financial systems by blackmailing or threatening staff;
– The threat of a targeted ransomware attack to disrupt the operation of the banking systems has increased, so improved security measures can be suggested, e.g. ransomware-proof data storage and appropriate security awareness;
– One expert from a Hungarian bank emphasized the importance of being protected against disinformation. A targeted disinformation campaign against relevant staff may result in disruption to the operation of banking services, hence the importance of resilience in the financial sector. Security awareness has been found to be one of the fundamentals of this type of resilience (Miyamoto, 2021), so an improved security awareness programme can be suggested within the banking industry.

Having examined the extra cyber challenges faced by the banking industry since the outbreak of the war, two questions can be posed: What may be the possible reasons behind the increased possibility of cyber-attacks? Can European banks really be the

subject of a targeted attack? As explained in the Introduction, information warfare operations are part of Russian military doctrine, so expecting the occurrence of it seems logical. Furthermore, circumventing the financial sanctions issued by the EU on Russia would be a possible motivation for attackers. Besides the risk of cyber-attacks targeting only the banking industry, the ICT systems of the banks could also be damaged by incidents which were originally targeting other sectors. A well-known example of this is the ransomware called 'notPetya', which caused damage to critical infrastructure outside Ukraine (Štrucl, 2022). Moreover, extremists could launch a cyber-attack against European critical infrastructure in order to provoke EU and NATO members to enter the war. A well-known example for this is the case of Kosice in 1941, when the bombing of the city by unidentified aircraft caused Hungary to enter WWII. As has been demonstrated above, some of the services of the banking industry can be considered essential, so European banks may be the potential targets of cyber-attacks.

So far, this paper has focused on the current cyber risks to the European banking industry. In the following section some recommendations will be given in order to increase the level of resilience and protection against these perfectly possible cyber-attacks.

4 ENHANCING INFORMATION SECURITY

All the aforementioned factors and data show that since the outbreak of the war cyber threats against critical infrastructure and especially against the banking sector have increased. However, a note of caution is due here, since only part of the data is available publicly.

Having examined the current cyber risks, some points can be suggested in order to enhance the level of information security. To be better prepared for cyber incidents and disruptive events, fostering the current public-private partnership has already been urged (Matyok and Zajc, 2020). Such a partnership may prove to be valuable in the following areas:

- Developing a common measurement system (e.g. as recommended by Roshanaei, 2021) to evaluate the risks, abilities and action plans is essential to any cooperation across private sectors and the defence sector. A commonly accepted maturity model (e.g. recommended by Sharkov, 2020) may also be suggested for cyber security and resilience at the EU level. As a further improvement, the European legislative framework must be enhanced. The main weaknesses of the current European cyber security strategy have already been highlighted (Bederna and Rajnai, 2022), and further studies must analyse the NIS 2 Directive of the EU, which is coming soon, in order to identify further points of improvement in the light of the ongoing war;
- Training is essential to develop a safety culture and increase the level of preparedness. Training should be planned appropriately (e.g. as suggested by

Young, 2022) and organized in cooperation with members of the financial sector, the relevant authorities and members of the defence sector. Any training is an opportunity for the experts to meet and develop professional relationships;
– Although tests and simulations are regularly held, these are organized individually. Tests, simulations and tabletop exercises should be organized for respective members of the financial sector and relevant bodies of the defence sector. The *Cyber Exercise Platform* of ENISA is an example of this concept; however, it could be further enhanced. The results of such tests may be fruitful for other sector members as well and, moreover, may trigger the necessary legislation process;
– Research & Development programmes should be commenced in cooperation with academic institutions. Further research is recommended on the concept of resilience and the measures of effectiveness (Fluri and Tagarev, 2020); exploring information warfare and cyber risks is also important.

A common measurement framework, training, test exercises and research programmes should be organized internationally, preferably at the level of the EU and NATO, in order to increase the ability to react together quickly in the event of a cyber-attack. The fruits of the EU-NATO strategic partnership have already been demonstrated (Štrucl, 2021); however, this cooperation should be further enhanced. Since the whole EU and NATO community may be a target in the future, and all the Member States may face the same cyber threats, Beckvard was right when he urged much more cooperation (Beckvard, 2022). Such international cooperation has also been suggested by the European Central Bank (Tuominen, 2022).

Conclusion

The information security of the banking industry is critical, since i) banking services play an essential role in the growth of the economy and well-being of people, and ii) the financial sanctions on Russia adopted by the EU are implemented and maintained by European banks. As has been shown with examples, being involved in the war, the European banks are facing an exceptionally high level of cyber risk due to the ongoing war in Ukraine. Any major disruption would have a negative impact on the economy of EU and NATO members and, moreover, would surely jeopardize the political stability and peace-building efforts of the West.

For these reasons, the cyber risks of the European Union's banking industry must be addressed appropriately. Based on our findings, the following steps can be recommended to further enhance information security in the EU's banking industry. Firstly, a common measurement framework should be developed in order to evaluate the risks, abilities and mitigating actions appropriately, together with a commonly accepted maturity model. Secondly, improved common training is fundamental for members of the banking industry and for law enforcement and defence bodies. Thirdly, joint test exercises for the banking industry and the defence sector are urged, in order to learn and work together. Finally, research programmes can be suggested at the EU and NATO level in order to better understand the security challenges and find the best answers in cooperation with sector specific authorities and the academic community.

References

1. *Ahmed, S., Hasan, M. M., and Kamal, M. R., 2022. Russia-Ukraine crisis: The effects on the European stock market. European Financial Management, pp 1-41.*
2. *Beckvard, H. P., 2022. Protecting critical infrastructure and critical information infrastructure. Contemporary Military Challenges, 24(2), pp 15-28.*
3. *Bederna, Zs., and Rajnai, Z., 2022. Analysis of the cybersecurity ecosystem in the European Union. International Cybersecurity Law Review, 3(1), pp 35-49.*
4. *Besenyő, J., 2008. A new kind of war? Internet warfare in Georgia. Army Review, 6(3), pp 61-63.*
5. *Besenyő, J., and Kovács, A. M., 2023. Healthcare cybersecurity threat context and mitigation opportunities. Security Science Journal., 4(1), 2023, pp 83-101.*
6. *Besenyő, J., Márton, K., and Schaffer, R., 2021. Hospital attacks since 9/11: an analysis of terrorism targeting healthcare facilities and workers. Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2021.1937821.*
7. *Blair, D.C., and Roth, W., 2022. Cyber Crime and Geostrategic Clash Over the Internet. The Cyber Defense Review, 7(2), pp 15-33.*
8. *Blank, S., 2008. Web War I: Is Europe's First Information War a New Kind of War? Comparative Strategy, Issue 27, pp 227-247.*
9. *Costigan, S., 2016. Cybersecurity, Global Governance and New Risk. In: India's Approach to Asia: Strategy, Geopolitics and Responsibility.*
10. *European Banking Authority (EBA), 2017. Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP). 11 May 2017. Available at: 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 (Accessed: 29 March 2023).*
11. *European Central Bank, 2021. Supervision newsletter, IT and Cyber Risk: A Constant Challenge. 18 August 2021. Available at: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2021/html/ssm.nl210818_3.en.html (Accessed: 8 April 2023).*
12. *European Central Bank, 2022a. FAQs on the Russia-Ukraine War and ECB Banking Supervision, 2022. Available at: https://www.bankingsupervision.europa.eu/press/publications/html/ssm.faq_Russia_Ukraine_war_and_Banking_Supervision~8360ccdf6f.en.html (Accessed: 8 April 2023).*
13. *European Central Bank, 2022b. Supervisors' Reaction to the War in Ukraine. Supervision Newsletter, 18 May, 2022. Available at: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl220518_1.en.html (Accessed: 8 April 2023).*
14. *Europol, 2020. Covid-19 Sparks Upward Trend in Cybercrime. Press release 5 October 2020. Available at: https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime (Accessed: 8 April 2023).*
15. *Fluri, P., and Tagarev, T., 2020. The concept of resilience: security implications and implementation challenges. Connections: The Quarterly Journal, 19(3), DOI: 10.11610/Connections.19.3.00.*
16. *Hugyik, A., 2020. Best Practices in the Application of the Concept of Resilience: Building Hybrid Warfare and Cybersecurity Capabilities in the Hungarian Defence Forces. Connections: The Quarterly Journal, 19(4) pp 25-38.*
17. *Information System Authority, Republic of Estonia, 2022. Trends and Challenges in Cyber Security. Quarterly Assessment, 2nd Quarter 2022.*
18. *Kenney, M., 2015. Cyber-Terrorism in a Post-Stuxnet World. Orbis, 59(1), pp 111-128.*
19. *Kohler, J. J., Fragnière, E., Konstantas, D., and Viganòet. E., 2021. Fictitious Crisis Scenario Development Related to a Bank Following a Breakdown in the Communication Network to Show Critical Infrastructure Digitization. International Journal of Future Computer and Communication, DOI: 10.18178/ijfcc.2021.10.2.574.*

20. *Matyok, T. and Zajc, S., 2020. Joint civil-military interactions as a tool in responding to hybrid threats. Contemporary Military Challenges, 22(3), pp 27-44.*
21. *Miyamoto, I., 2021. Disinformation: policy responses to building citizen resiliency. Connections: The Quarterly Journal, 20(2), pp 47-55.*
22. *Nagy, R. and Somogyi, T., 2021. Financial infrastructure as a critical infrastructure and its specialities. National Security Review, Issue 2, pp 207-217.*
23. *National Bank of Hungary, 2022. EBA calls on financial institutions to ensure compliance with sanctions against Russia following the invasion of Ukraine and to facilitate access to basic payment accounts for refugees. Press release, 11 March 2022. Available at: https://www.mnb.hu/en/pressroom/press-releases/press-releases-2022/eba-calls-on-financial-institutions-to-ensure-compliance-with-sanctions-against-russia-following-the-invasion-of-ukraine-and-to-facilitate-access-to-basic-payment-accounts-for-refugees (Accessed: 8 April 2023).*
24. *Pallin, C. V., and Westerlund, F., 2009. Russia's war in Georgia: lessons and consequences. Small Wars and Insurgencies, 20(2), pp 400-424.*
25. *Plėta, T., Ivaronavičienė, M., Della Casa, S., and Agafonov, K., 2020. Cyber-attacks on critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development, 2(3), pp 703-715.*
26. *Rácz, A., 2020. The effects of World War I on marriages between 1914 and 1918 in Hungary. Belvedere Meridionale. 32(3), pp 115-122.*
27. *Reveron, D. S., and Savage, J.E., 2020. Cybersecurity Convergence: Digital Human and National Security. Orbis, 64(4), pp 555-570.*
28. *Roshanaei, M., 2021. Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. Journal of Computer and Communications, 9(8), pp 80-102.*
29. *Sharkov, G., 2020. Assessing the maturity of national cybersecurity. Connections: The Quarterly Journal, 19(4), pp 5-24.*
30. *Somogyi, T., and Nagy, R., 2022. Cyber threats and security challenges in the Hungarian financial sector. Contemporary Military Challenges, 24(3), pp 15-29.*
31. *Štrucl, D., 2021. The EU-NATO partnership and ensuring information security and cybersecurity: theory and practice. Contemporary Military Challenges, 23(2), pp 29-47.*
32. *Štrucl, D., 2022. Russian aggression on Ukraine: cyber operations and the influence of cyber space on modern warfare. Contemporary Military Challenges, 24(2), pp 103-123.*
33. *Tuominen, A., 2022. The resilience of the European banking sector. Conference speech. Florence School of Banking and Finance's Annual Conference. 14 June 2022. Available at: https://www.bankingsupervision.europa.eu/press/speeches/date/2022/html/ssm.sp220614~f5ea7887ec.en.html (Accessed: 8 April 2023).*
34. *Young, C., 2022. Planning for success: a call to optimize NATO cyber training. Contemporary Military Challenges. 24(2), pp 29-48.*
35. *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, 4(3), pp 80-87.*

email: somogyi.tamas@phd.uni-obuda.hu

ORCID: 0000-0003-1397-697X

email: nagy.rudolf@bgk.uni-obuda.hu

ORCID: 0000-0001-5108-9728

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

Mag. Tamás Somogyi je magistriral iz informacijskega inženiringa in dodatno še iz pravnih študij. V bančništvu je zaposlen od leta 2007. Trenutno je doktorski študent na doktorski šoli za varstvoslovje na univerzi Óbuda. Raziskovalno se ukvarja z varnostnimi vprašanji infrastrukture finančnega sektorja**.**

Tamás Somogyi, MSc, holds a Master's degree in IT engineering and a complementary degree in Legal Studies. He has been working in the banking industry since 2007. He is currently a PhD student at the Doctoral School on Safety and Security Sciences, Óbuda University. His research area is the security issues of the financial sector's infrastructure**.**

ORCID: 0000-0003-1397-697X

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

Dr. Rudolf Nagy, polkovnik v pokoju, je habilitiran 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 na 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.

Colonel (Ret) Rudolf Nagy, PhD, is a habilitated Assistant Professor at Óbuda University. He was a CBRN defence engineer 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 the Hungarian National Directorate General for Disaster Management. He has been teaching subjects of safety and security sciences since 2015.

ORCID: 0000-0001-5108-9728