DOI: 10.53477/1842-9904-24-17

TERRORIST ATTACKS AGAINST THE EUROPEAN BANKING INDUSTRY SINCE 2001

Tamas SOMOGYI*
Rudolf NAGY**

There is a growing body of literature that recognises the importance of counter-terrorism and security, especially after the events of 9/11. Studies of terrorism and critical infrastructure protection agree on the essential nature of financial services and mention many cases when banks were attacked. However, the threat of terrorism to the banking industry received scant attention. This is the first study set out to investigate the terrorist attacks against banks in Europe since 2001. Research data were collected from the Global Terrorism Database.

The aim of this quantitative research is to i) examine the terrorist attacks against European banks over the last two decades, ii) identify trends and patterns, and iii) provide some recommendations to increase the level of resilience.

Our findings and recommendations can bring important contributions to the field of counter-terrorism and security. The study may hold relevance for researchers, operators of essential services, law enforcement agencies and policy-makers.

Keywords**:** *Europe; banking industry; bank; terrorism; terrorist attack; Global Terrorism Database; critical infrastructure protection.*

Introduction

The significance of essential services can be understood by its definition provided by the EU Directive 2022/2557, Article 2: "a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment". Generally, transport (Shatnawi and Rajnai 2023), services of

**** Tamas SOMOGYI, MSc, is a PhD Student at the Doctoral School of Safety and Security Sciences, Óbuda University, Budapest, Hungary. E-mail: somogyi.tamas@phd.uni-obuda.hu***
***** Colonel (Ret) Rudolf NAGY, PhD, is a habilitated Assistant Professor at Doctoral School of Safety and Security Sciences, Óbuda University, Budapest, Hungary. E-mail: nagy.rudolf@bgk.uni-obuda.hu***

the energy sector (Yusta et al. 2011), the healthcare system (Shaffer and Besenyő 2023), food production (Wu and Takács-György 2023), the water sector (Berek 2024) and the banking industry (Pursiainen and Kytömaa 2023) are considered essential. The critical infrastructure that provides these essential services, undoubtedly plays a vital role in our society. Therefore, protecting critical infrastructure is a fundamental (Fjäder 2014). Although the idea of protecting important places and objects is absolutely not a new one (e.g., the European explorers established fortified towns to secure their commercial interests on the shores of Africa (Besenyő 2017)), in the last decades this topic is receiving more and more attention.

The smooth operation of critical infrastructure is jeopardised by natural hazards and man-made hazards (Faramondi et al. 2020). For instance, the effects of global warming are a major concern within the former category (Somogyi and Nagy 2022), while terrorism is central to the latter group (Asmer et al. 2019; Besenyő and Sinkó 2024). Protecting the infrastructure from the intentional man-made attacks is a major area of interest within the field of security (Szabó and Balogh 2021). Cyber security (Haya and Rajnai 2023), physical security (Novák 2021), and counter-terrorism (Cross 2023) are extensively studied nowadays. The field of security and military science has been developed to a highly investigated multidisciplinary field (Vuk 2023; Szűcs and Szakali 2023). Divišová et al. (2023) has suggested that the public expectation is that states and armed forces be capable to deal with hybrid interference, including terrorism.

By playing an important role and providing essential service, the banking industry obviously has to be protected against terrorist attacks. The aim of this paper is to examine the terrorist attacks against banks and provide some recommendations to increase the level of resilience.

Methodology

The study set out to investigate the terrorist attacks against European banks. It was decided that the best source of data for this research is the Global Terrorism Database (GTD). GTD is an event-level database in English, containing more than 200,000 records of terrorist attacks that have been taking place around the world since 1970[1]. Another advantage of GTD is its reliability: it has been used in several researches, e.g., Jasani et al. (2023) and Guohui et al. (2014).

Terrorist attacks were only included in the analysis provided:

- The year they took place is not before 2002,
- The region is “Eastern Europe” or “Western Europe”,
- The Target/Victim Subtype is “Bank/Commerce”.

[1] The database is available online at URL: https://www.start.umd.edu/gtd

To identify events related to banks, the field "Incident summary" was used. There have been found 153 cases of terrorist attacks against the European banking industry. These cases have been examined in our research.

1. The Threat of Terrorism to Critical Infrastructure

Mirza and Rana (2024) found that the number of studies on terrorism had been increased after the 9/11 attacks in 2001. Thus, nowadays there is a growing interest in the field of terrorism and counter-terrorism. What is terrorism and why is it important for the field of critical infrastructure protection? Terrorism is considered to be severe violence committed by radicalised people for the purpose of achieving extreme political goals (Prezelj et al. 2018). Papamichael et al. (2024) noted that research on critical infrastructure protection has multiplied after high-profile terrorist attacks.

But does terrorism really impose a threat to critical infrastructure? By analysing the situation in the Middle-East, Khan (2024) pointed out that terrorism jeopardises the operation of infrastructure and negatively affects the economy by the devastation of infrastructure and interrupting the services and commercial operations. Glickman (2008) identified terrorism as an enormous challenge to critical infrastructure protection. It has been assumed that critical infrastructure will be terrorists' target in the future as well (Jenelius et al. 2010). Due to the so-called cascading effect, disruption of a sector may have an effect on other essential services as well (Sellevåg 2021). Financial services illustrate this cascading effect: operators of essential services naturally rely on the services of the banking industry. Therefore, for terrorists, causing outage of essential services can be an aim, but it is highly likely that critical infrastructure will be targeted.

Several analysis of terrorist attacks have found that attacks can either be simple, cheap, low-cost attacks or complex and costly ones. A case study of the energy sector was able to demonstrate that attackers can cause serious damage with simple tools and explosives (Eze et al. 2017). Besenyő (2021) has mentioned cases when terrorists attacked hospitals with knives, baseball bats and stones. On the other hand, terrorism has also been identified as a threat that has to be covered by information security (Theoharidou et al. 2008). Technology has been found as a tool used by terrorists to provide information, solicit financial support, connect with others, recruit and gather information (Quigley et al. 2015). It has been demonstrated that terrorist groups are actively using the internet and social media for their malicious activities (Besenyő and Sinkó 2021). Moreover, some of the terrorist groups even have their own secret service (Sinkó and Besenyő 2024) which clearly shows their potential and capabilities. Marx et al. (2024) have suggested that the two major terror threats to hospitals are the attacks with conventional weapons and cyber-attacks. According to Chen et al. (2011), the technological development and terrorism clearly show

the fragility of our society. It should be mentioned that some terrorist groups are supported by states (Kocjančič 2023). Terrorism can be an integrated part of the so-called proxy war (Boda 2023), therefore, some of the terrorist groups can have financial support and technology to carry out a high-level attack against critical infrastructure. These results highlight the importance of protecting critical infrastructure.

Analysing the terrorism in Cabo Delgado, Besenyő and Hegedűs (2024) demonstrated that banks were attacked as the infrastructure of financial services were also targeted by terrorists. The motivations of terrorist attacks on the banking industry may vary, but certainly there is the goal of disseminating fear, causing mass confusion and causing financial loss. Beside the financial loss due to the obvious physical damage, it has been proved that terrorism decrease the GDP per capita (Paul and Bagchi 2023). Conflicts and terrorism negatively affect businesses and investments. Attacking banks and business can lead to these desired results, especially if the above-mentioned cascading effect is taken into consideration. The outage of the banking services may cause liquidity problems in other critical sectors and can lead to political instability. Moreover, Posso (2023) has demonstrated that in regions hit by terrorism and armed conflict, people tend to choose informal financial services, which are considered less vulnerable to conflict and terrorism. A connection has been established between the uncontrolled, informal financial services, e.g., hawala, and the finance of terrorism and money laundering (Somogyi and Nagy 2023a). Moreover, legislative controls over the services of the banking industry are an integral part of counter-terrorism (Jirásek 2023). Another possible motivation for terrorists to cause (financial) instability by targeting critical infrastructure is connected to migration. A link has been established between migration generated by instability and terrorist groups who are engaged in human trafficking (Nagy et al. 2023). Overall, these findings underline that essential services, including financial services, need to be secured against terrorist attacks.

Previous studies have demonstrated the increasing threat of terrorism to critical infrastructure and have suggested a continuing trend. Beside the conventional weapons, the usage of modern technology for terrorist activities also has been shown. Hence the importance of advancing the knowledge on terrorism and contributing to the field of critical infrastructure protection, including the banking industry. Having discussed the threat of terrorism to critical infrastructure, the following part will examine the terrorist attacks on the banking industry.

2. Terrorist Attacks against the European Banking Industry - Research Results

The Global Terrorism Database (GTD) has been queried as described in the Methodology. In the result, 153 terrorist attacks were identified and all of them were categorised into four groups. The two major categories are the *bombing/explosion*

and the *facility/infrastructure attack*. There are two small categories as well, the *armed assault* and the *hostage taking*. These category names are used in the attack type field in the GTD. Quotations in the following pages are taken from the Summary field that contains the summary of the incident.

The biggest group of terrorist attacks against banks is the facility/infrastructure attack. In 79 cases out of 153, a facility or infrastructure has been attacked. For instance, in Thessaloniki, Greece, on May 27, 2008, "an incendiary device was thrown at the Millennium bank subsidiary in Thessaloniki, Greece by unknown anarchists". Another example is the attack on October 16, 2017, when "an assailant set fire to a Banque de France branch in Place de la Bastille, Paris, France". Another reported case happened in Oiartzun, Spain, on May 24, 2003, when one of the BBVA bank's ATM machines "was burnt after radicals threw two Molotov cocktail at the machine". Beside these individual cases, there were attacks that are linked to each other by the authorities. An example in this regard is the series of events which happened on February 17, 2006, when "suspected anarchists used homemade incendiary devices in five arson attacks targeting banks, which occurred within 30 minutes of one another, in the greater Athens area of Greece". Another reported case refer to the three attacks on April 3, 2006, when three Turkish bank branches damaged in an overnight gasoline-bomb attack in Northern London, UK. A similar event took place on December 13, 2020, when "assailants threw a Molotov cocktail at a Hellenic Bank branch in Agia Fyla, Limassol, Cyprus" as part of two related attacks. Perhaps the biggest coordinated terrorist attacks against banks happened on November 30, 2014, when assailants set fire to seven ATMs in Athens, Greece, on the same day. Out of 79 facility/infrastructure attacks, 58 terrorist attacks are parts of related events, and only 21 cases are considered individual cases. Whether individual cases or not, in all cases facility damages were reported but no serious injury or death occurred. This is due to the fact, that in most of the cases, the attacks were outside of the opening hours, mostly at night or early in the morning.

The second category of the terrorist attacks against the banking industry is the bombing/explosion. It includes 67 cases out of the total of 153 attacks targeting banks. Explosives are used in these cases, e.g., on January 16, 2008, when a bank damaged in a bomb attack in Bastia, Corsica, France. Another example happened on April 25, 2016, when "assailants fired a rocket launcher at a Pivdennyi Bank building in Odesa, Ukraine". Home-made devices are also used, for instance on May 13, 2002, when "two camping gas cylinders and several lead balls exploded at a La Caixa Bank cash dispenser in Barcelona, Spain". In most of the cases the attackers could not be identified, however, in some cases, it was important for the terrorists to identify themselves. The following case clearly illustrates this. On April 10, 2018, "an explosive device detonated at a UniCredit bank in Bologna, Italy. Anarchists claimed responsibility for the incident in a note left at the scene criticising Turkish

President Recep Tayyip Erdogan". These cases were individual ones, however, there are many coordinated series of attacks. Out of the total of 67 attacks in this category, 23 cases were part of a series of attacks. The following case is a good illustration of the coordinated attacks. On October 17, 2002, a week before Interior Minister Nicolas Sarkozy was scheduled to arrive, 14 explosions occurred throughout the night at various towns in Corsica, including four banks in Ghisonaccia, Corsica, France. A similar case occurred on January 21, 2008, when "unknown perpetrators detonated home-made bombs next to 6 banks, 22 vehicles and 3 luxury car showrooms in Athens and Salonica, Greece". Another example is the case reported on January 24, 2013, when an explosive device detonated near a Credit Suisse bank branch in Zurich, Switzerland, as one of the two attacks in protest of the World Economic Forum. Interestingly, in the majority of the attacks, in the category of bombing/explosion, no serious injury or death was reported. This is due to the fact that these attacks were either carried out during non-working hours or terrorist paid attention to the people nearby. An example for the former type of attack is the case on the April 11, 2009, when "explosive device exploded outside an office building that houses an Alpha Bank branch and the offices of the Cetelem Insurance company" on Saturday night at 04:15. The following case in Newry, Northern Ireland clearly shows how terrorists took care of the people in order to avoid injuries. On August 22, 2011, two Irish nationalists carried a bomb concealed in a bag into a Santander Bank branch and shouted that the device would detonate in 45 minutes and then escaped on foot. The British army defused the bomb in time. It is clear that the attackers wanted to avoid injuries in Athens, Greece, as well, when on February 16, 2010, a time-bomb exploded outside a JP Morgan bank at 19:50. "Shortly before the bombing, a local newspaper received a warning call and in turn immediately informed the police", so the area could be cordoned off in time.

These were the two major categories of the terrorist attacks (the bombing/explosion and the facility/infrastructure attack), and there are two small categories: the armed assault and the hostage taking. The result from the GTD contains two hostage taking cases and five armed assault cases as well. The two hostage takings were individual cases with no casualties, both of them are reported from Ukraine. The five reported armed assault attacks also ended without casualties. On April 28, 2014, assailants opened fire on a bank branch in Donetsk city, Ukraine, but did not cause any harm to anyone. The remaining four armed assault cases occurred on the January 1st, 2002, when "approximately 40 hooded assailants hurled Molotov cocktails and other incendiary devices at four Spanish banks in Guernica, Spain", and also "assaulted local police patrols responding to the scene".

Having explore the terrorist attacks by their categories, it is now necessary to examine the number of attacks by year in order to identify trends. Table no.1 shows the number of terrorist attacks against the European banking industry by year. Interestingly, there are significant differences between the number of cases over time.

Table no. 1: Number of terrorist attacks against the European banking industry, by year[2]

Year	Facility/ Infrastructure attack	Bombing/ Explosion	Total number of attacks
2002	3	9	16
2003	7	0	7
2004	0	2	2
2005	0	2	2
2006	9	6	15
2007	1	4	5
2008	17	7	24
2009	14	5	19
2010	1	2	3
2011	0	2	2
2012	0	3	3
2013	2	4	6
2014	10	5	17
2015	3	9	12
2016	3	2	5
2017	4	2	6
2018	0	1	1
2019	0	2	2
2020	5	0	6
2021	0	0	0

In summary, the GTD contains 153 terrorist attacks against banks or ATMs, of which in the most cases are either bombing/explosion or facility/infrastructure attack. Although in some cases the physical damage is significant, no death or serious injury has been reported. The next section discusses our findings based on these 153 cases.

3. Discussion

The current study found that terrorists have attacked the European banking industry 153 times since 2001. This is the most important finding, it further supports that banks are threatened by terrorism. The reported cases clearly show that the main goal is not killing or causing injuries but causing damage to the infrastructure. This seems to be consistent with the literature reviewed in the beginning of this

[2] Source: edited by the authors based on the GTD

paper, suggesting that terrorism jeopardises the critical infrastructure. The cases also confirm that terrorist activities have political goals. The above-mentioned attacks in Corsica in 2002 and in Bologna in 2018 were clearly politically motivated terrorist attacks. Therefore, in general, it seems that banks and ATMs are attractive targets for terrorists. Taking into consideration that terrorism may increase in Europe, it is probable that terrorist attacks against the European banking industry will continue in the future.

Thus, a question arises, namely "It is possible to identify patterns or tendencies that have emerged over the past two decades?" The number of terrorist attacks by year (Table no. 1) shows differences between the years. There were years with only a few cases, but periodically there is a sharp rise. With a small sample of two decades, caution must be applied, however, it is likely that terrorist attacks against banks rise in every six years or so. It is important to bear in mind that the war in Ukraine affects the security in Europe (e.g., Štrucl 2022; Somogyi and Nagy 2023b), therefore a shift in this period is possible. Nevertheless, it is necessary to be prepared for further terrorist attacks against the banking industry.

These findings may be somewhat limited by the data of GTD. The database is believed to be accurate, however, it is possible that cases are missing from the database that were not identified as terrorist attacks, but were committed by terrorists (e.g., bankrobbery in order to make money for their malicious activities).

After providing insights into the terrorist attacks, some recommendations can be given. As the most important result is that terrorism poses a serious threat to the banking industry, the first recommendation is that more research is needed to support the efforts of counter-terrorism and critical infrastructure protection. Although the reported cases show that killing or causing injuries was not an intention in the past, it may change in the future. Galehan (2019) has pointed out that the terrorist group Boko Haram took advantage of women, using them in suicide bombings. Therefore, it can also be recommended to make the necessary preparation against bombing attacks during working hours. The consequences of killing and causing injuries by bombing an open bank branch would be serious. In addition to this, data clearly shows that some European countries suffer much from terrorist attacks, e.g., Greece, Spain and the UK. Exploring ways of effective international cooperation on sharing information, training and research can also be recommended. Such cooperation may be incentivised on EU level, e.g., by the European Central Bank.

Conclusion

Based on the literature, there are reasons to suggest that terrorist groups target the banking industry worldwide. This study set out to investigate the terrorist attacks against banks in Europe by analysing the cases recorded in Global Terrorism Database.

The results of our research could underpin that European banks are jeopardised. This study has found that the vast majority of terrorist attacks over the last two decades were targeted the infrastructure outside of the working hours, thus no death or serious injury reported. Examining the number of attacks by years, a pattern has also been identified: there is a sharp rise in terrorist attacks periodically. Therefore, it is highly probable that similar incidents will continue to occur in the upcoming years.

Taken together, these findings suggest that more research and actions are needed. To support this, three recommendations were provided in this study: i) further studies which take into account the threat of terrorism to the banking industry; ii) make the necessary preparation for being protected against bombing attacks during working hours; iii) explore ways of effective international cooperation on sharing information, training and research.

This study highlighted our understanding of terrorism and its impact, and also the importance of protecting critical infrastructure which incorporates the banking industry. Our findings and recommendations are relevant to researchers, operators of essential services, law enforcement agencies and policy-makers.

BIBLIOGRAPHY:

Asmer, L., Popa, A., Koch, T., Deutschmann, A. and Hellmann, M. 2019. "Secure rail station – Research on the effect of security checks on passenger flow". *Journal of Rail Transport Planning & Management* 10: 9–22. https://doi.org/10.1016/j.jrtpm.2019.04.002

Berek, T. 2024. "Integrated Physical Protection of Emergency Water Production Facilities". In: Kovács, Tünde Anna; Nyikes, Zoltán; Berek, Tamás; Daruka, Norbert; Tóth, László (eds.) *Critical Infrastructure Protection in the Light of the Armed Conflicts* Cham, Svájc : Springer Nature Switzerland AG (2024) pp. 329-340. https://doi.org/10.1007/978-3-031-47990-8_29

Besenyő, J. 2021. "Terror attacks against African health facilities". In: Florian, CÎRCIUMARU and Constantin-Crăișor, IONIȚĂ (eds.) *Proceedings: International Scientific Conference Strategies XXI - The Complex and Dynamic Nature of The Security Environment*, Bucharest, Romania: Carol I National Defence University Publishing House (2022) pp. 66-74. https://cssas.unap.ro/en/pdf_books/conference_2021.pdf

Besenyő, J. 2022. "Portugal's Forgotten Overseas Wars in the 20th Century: Review article." *Terrorism and Political Violence* 34(1): 189–194. https://doi.org/10.1080/09546553.2021.2017164

Besenyő, J. and Hegedűs, É. 2024. "Countering Extremist Violence and Terrorism in Cabo Delgado: (How) Can Past Peace-Building and DDR Lessons Be of Use?". *Journal of Central and Eastern European African Studies* 3(4): 139–161. https://doi.org/10.59569/jceeas.2023.3.4.244

Besenyő, J. and Sinkó, G. 2021. "The social media use of African terrorist organizations: a comparative study of Al-Qaeda in the Islamic Maghreb, Al-Shabaab and Boko Haram". *Insights into Regional Development* 3(3): 66-78. https://doi.org/10.9770/ird.2021.3.3(4)

Besenyő, J. and Sinkó, G. 2024. "Terrorist Organizations' Activities Against Crucial Installations: Al-Shabaab's Attacks on Critical Infrastructure in Kenya". In: Besenyő, J., Khanyile, M.B., Vogel, D. (eds.) *Terrorism and Counter-Terrorism in Modern Sub-Saharan Africa*, Cham, Springer Nature Switzerland (2024) pp. 169-193. https://doi.org/10.1007/978-3-031-56673-8_8

Boda, M. 2023. "Proxy War: Its Philosophy and Ethics". *Contemporary Military Challenges* 25(3-4): 9-21. https://doi.org/10.2478/cmc-2023-0019

Chen, J. et al. 2011. "A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection". *Journal of Network and Computer Applications* 34(4): 1225-1239. https://doi.org./10.1016/j.jnca.2011.01.008

Cross, M.K.D. 2023. "Counter-terrorism & the intelligence network in Europe". *International Journal of Law, Crime and Justice* 72 https://doi.org/10.1016/j.ijlcj.2019.100368

Divišová, V., Frank, L. and Bízik, V. 2023. "A resilient soldier, a resilient state - A Tool for Measuring Czech Armed Forces' Resilience Against Hybrid Interference". *Obrana a strategie (Defence & Strategy)* 23(1): 173-191. http://dx.doi.org/10.3849/1802-7199.23.2023.01.173-191

Eze, J., Nwagboso, C. and Georgakis, P. 2017. "Framework for integrated oil pipeline monitoring and incident mitigation systems". *Robotics and Computer–Integrated Manufacturing* 47: 44-52. http://dx.doi.org/10.1016/j.rcim.2016.12.007

Faramondi, L., Oliva, G. and Setola, R. 2020. "Multi-criteria node criticality assessment framework for critical infrastructure networks". *International Journal of Critical Infrastructure Protection* 28 https://doi.org/10.1016/j.ijcip.2020.100338

Fjäder, C. 2014. "The nation-state, national security and resilience in the age of globalisation". *Resilience* 2(2): 114-129. https://doi.org/10.1080/21693293.2014.914771

Galehan, J. 2019. "Instruments of violence: Female suicide bombers of Boko Haram". *International Journal of Law, Crime and Justice* 58: 113-123. https://doi.org/10.1016/j.ijlcj.2019.04.001

Glickman, T. 2008. "Program portfolio selection for reducing prioritized security risks". *European Journal of Operational Research* 190: 268–276. https://doi.org/10.1016/j.ejor.2007.06.006

Guohui, L. et al. 2014. "Study on Correlation Factors that Influence Terrorist Attack Fatalities Using Global Terrorism Database". *Procedia Engineering* 84: 698-707. https://doi.org/10.1016/j.proeng.2014.10.475

Haya, A. and Rajnai, Z. 2023. "Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures" In: Szakál, A. (ed.) *SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics*, Budapest, Hungary: IEEE Hungary Section (2023) pp. 625-629. https://doi.org/10.1109/SISY60376.2023.10417951

Jasani, G., Alfalasi, R. and Liang, S. 2023. "Terrorist attacks against emergency departments". *The American Journal of Emergency Medicine* 64: 43-45. https://doi.org/10.1016/j.ajem.2022.11.011

Jenelius, E., Westin, J. and Holmgren, Å. 2010. "Critical infrastructure protection under imperfect attacker perception". *International Journal of Critical Infrastructure Protection* 3(1): 16-26. https://doi.org/10.1016/j.ijcip.2009.10.002

Jirásek, D. 2023. "Response of Kenya Security Forces to Terrorist Attacks in the Post-Westgate Period". *Obrana a strategie (Defence & Strategy)* 23(2): 3-21. https://doi.org/10.3849/1802-7199.23.2023.02.003-021

Khan, H.U. 2024. "An analytical investigation of consequences of terrorism in the Middle East". *Journal of Economic Criminology* 4 https://doi.org/10.1016/j.jeconc.2024.100067

Kocjančič, K. 2023. "Analysis of the Armed Conflict: A Case Study of Lord's Resistance Army". *Contemporary Military Challenges* 25(3-4): 51-65. https://doi.org/10.2478/cmc-2023-0022

Marx, J., Leroy, C., Philippe, J. and Vivien, B. 2024. "L'hôpital attaqué". *La Presse Médicale Formation* 5(3): 225-231. https://doi.org/10.1016/j.lpmfor.2024.04.003

Mirza, M.N.E. and Rana, I.A. 2024. "A systematic review of urban terrorism literature: Root causes, thematic trends, and future directions". *Journal of Safety Science and Resilience* 5: 249–265. https://doi.org/10.1016/j.jnlssr.2024.03.006

Nagy, R., Bérczi, L., Sáfár, B. and Kállai, K. 2023. "The Relationship of Environmental Migration and Human Trafficking Concerning Natural Hazards at the Affected Regions of Africa". *Journal of Central and Eastern European African Studies* 3(1): 17-46. https://doi.org/10.59569/jceeas.2023.3.1.209

Novák, A. 2021. "International physical barriers along the Balkan Migration route". *National Security Review*, Issue 1: 87-112. https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_1_NSR.pdf#page=87

Papamichael, M., Dimopoulos, C. and Boustras, G. 2024. "Performing risk assessment for critical infrastructure protection: an investigation of transnational challenges and human decision-making considerations". *Sustainable and Resilient Infrastructure* https://doi.org/10.1080/23789689.2024.2340368

Paul, J.A. and Bagchi, A. 2023. "Immigration, terrorism, and the economy". *Journal of Policy Modeling* 45(3): 538-551. https://doi.org/10.1016/j.jpolmod.2023.03.002

Posso, A. 2023. "Terrorism, banking, and informal savings: Evidence from Nigeria". *Journal of Banking & Finance* 150 https://doi.org/10.1016/j.jbankfin.2023.106822

Prezelj, I., Kocjančič, K. and Marinšek, U. 2018. "Islamist Radicalisation Towards Extreme Violence and Terrorism". *Šolsko polje* 29(5-6): 85-106. https://www.pei.si/ISSN/1581_6044/5-6-2018/1581_6044_5-6-2018.pdf

Pursiainen, C. and Kytömaa, E. 2023. "From European critical infrastructure protection to the resilience of European critical entities: what does it mean?" *Sustainable and Resilient Infrastructure* 8(sup1): 85-101. https://doi.org/10.1080/23789689.2022.2128562

Quigley, K., Burns, C. and Stallard, K. 2015. "'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection". *Government Information Quarterly* 32 http://dx.doi.org/10.1016/j.giq.2015.02.001

Sellevåg, S.R. 2021. "Changes in inoperability for interdependent industry sectors in Norway from 2012 to 2017". *International Journal of Critical Infrastructure Protection* 32 https://doi.org/10.1016/j.ijcip.2020.100405

Shaffer, R. and Besenyő, J. 2023. "Terrorism against healthcare facilities and workers in Africa: An assessment of attack modes, targets and locations". *African Security Review* 32(3): 311-331. https://doi.org/10.1080/10246029.2023.2213220

Shatnawi, M. and Rajnai, Z. 2023. "Assessment of the impact of the COVID-19 crisis on transportation and mobility – analysis of applied restrictions" *Interdisciplinary Description of Complex Systems* 21(4): 365-374. https://doi.org/10.7906/indecs.21.4.6

Sinkó, G. and Besenyő, J. 2024. "More than Survival: The Role of al-Shabaab Secret Service, Amniyat, in Information-Gathering". *Connections QJ* 22(1): 99-111. https://doi.org/10.11610/Connections.22.1.36

Somogyi, T. and Nagy, R. 2022. "Some impacts of global warming on critical infrastructure protection - heat waves and the European financial sector". *Insights into Regional Development* 4(4): 11-20. https://doi.org/10.9770/IRD.2022.4.4%281%29

Somogyi, T. and Nagy, R. 2023a. "Formal banking and financial inclusion to weaken hawala and serve counter-terrorism" *National Security Review* Issue 2: 19-32. https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_2_NSR.pdf

Somogyi, T. and Nagy, R. 2023b. "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." *Contemporary Military Challenges* 25(3-4): 23-32. https://doi.org/10.2478/cmc-2023-0020

Štrucl, D. 2022. "Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare". *Contemporary Military Challenges* 24(2): 103-123. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6

Szabó, L. and Balogh, Zs. 2021. "Preventive measures of infrastructures" *Strategic Impact* 80(3) https://doi.org/10.53477/1841-5784-21-16

Szűcs, L. and Szakali, M. 2023. "Complex security challenges – complex responses" *Strategic Impact* 87(2) https://doi.org/10.53477/1842-9904-23-10

Theoharidou, M., Xidara, D. and Gritzalis, D. 2008. "A CBK for Information Security and Critical Information and Communication Infrastructure Protection". *International Journal of Critical Infrastructure Protection* 1: 81-96. https://doi.org/10.1016/j.ijcip.2008.08.007

Yusta, J.M., Correa, G.J. and Lacal-Arántegui, R. 2011. "Methodologies and applications for critical infrastructure protection: State-of-the-art". *Energy Policy* 39: 6100–6119. https://doi.org/10.1016/j.enpol.2011.07.010

Vuk, P. 2023. "Military Science and Educational Institutions" *Contemporary Military Challenges* 25(2): 9-26. https://doi.org/10.2478/cmc-2023-0011

Wu, Y. and Takács-György, K. 2023. "Why does food loss and waste matter for food security - from the perspective of cause and magnitude". *Ecocycles* 9(3): 47-61. https://doi.org/10.19040/ecocycles.v9i3.337